

EXHIBIT A

WILMER CUTLER PICKERING
HALE AND DORR LLP

SONAL N. MEHTA (SBN 222086)
Sonal.Mehta@wilmerhale.com
2600 El Camino Real, Suite 400
Palo Alto, California 94306
Telephone: (650) 858-6000

DAVID Z. GRINGER (*pro hac vice*)
David.Gringer@wilmerhale.com
7 World Trade Center
250 Greenwich Street
New York, New York 10007
Telephone: (212) 230-8800

ARI HOLTZBLATT (*pro hac vice*)
Ari.Holtzblatt@wilmerhale.com
MOLLY M. JENNINGS (*pro hac vice*)
Molly.Jennings@wilmerhale.com
1875 Pennsylvania Avenue, NW
Washington, District of Columbia 20006
Telephone: (202) 663-6000

Attorneys for Defendant Meta Platforms, Inc.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

MAXIMILIAN KLEIN, et al., on behalf of
themselves and all others similarly situated,

Plaintiffs,

v.

META PLATFORMS, INC., a Delaware
Corporation headquartered in California,

Defendant.

Case No. 3:20-cv-08570-JD

**LETTER OF REQUEST FOR
INTERNATIONAL JUDICIAL
ASSISTANCE PURSUANT TO THE
HAGUE CONVENTION OF 18 MARCH
1970 ON THE TAKING OF EVIDENCE
ABROAD IN CIVIL OR COMMERCIAL
MATTERS**

Judge: Hon. James Donato

1 The United States District Court for the Northern District of California presents its
2 compliments to the Registrar of the Supreme Court of the British Virgin Islands and requests
3 assistance in obtaining evidence to be used in civil proceedings before this Court.

4 This request is made pursuant to, and in conformity with, Chapters I and II of the
5 Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters
6 (the “Hague Evidence Convention”), to which both the United States and the British Virgin Islands
7 are party.

8 Specifically, the District Court requests assistance through the law firm Harney Westwood
9 & Riegels, LP of Craigmuir Chambers, P.O. Box 71, Road Town, Tortola, British Virgin Islands,
10 in obtaining evidence from non-party Telegram Messenger, Inc. (“Telegram”), a British Virgin
11 Islands (“BVI”) entity registered in Tortola, the British Virgin Islands.

12 **SECTION I**

13 **1. SENDER:**

14 The Honorable James Donato
15 United States District Court of the Northern District of California
16 450 Golden Gate Avenue
17 San Francisco, CA 94102
18 United States of America

19 **2. CENTRAL AUTHORITY OF THE REQUESTED STATE:**

20 Registrar of the Eastern Caribbean Supreme Court
21 Supreme Court Registry
22 Sakal Place, 2nd Floor
23 P.O. Box 418
24 Road Town, Tortola
25 British Virgin Island VG1110
26 Tel: +284 468 5001
27 Fax: +284 468 4951

28 **3. PERSON TO WHOM THE EXECUTED REQUEST IS TO BE RETURNED:**

The Honorable James Donato
United States District Court of the Northern District of California
450 Golden Gate Avenue
San Francisco, CA 94102
United States of America

With a Copy to the Parties' Legal Representatives:

Stephen A. Swedlow
Quinn Emanuel Urquhart & Sullivan, LLP
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Tel: (312) 705-7400
Email: stephenswedlow@quinnemanuel.com

Shana E. Scarlett
Hagens Berman Sobol Shapiro LLP
715 Hearst Avenue, Suite 202
Berkeley, CA 94710
Tel: (510) 725-3000
Email: shanas@hbsslaw.com

Yavar Bathaee
Bathaee Dunne LLP
445 Park Avenue, 9th Floor
New York, NY 10022
Tel: (332) 322-8835
Email: yavar@bathaeedunne.com

Kristen M. Anderson
Scott+Scott Attorneys at Law LLP
230 Park Avenue, 17th Floor
New York, NY 10169
Tel: (212) 223-6444
Email: kanderson@scott-scott.com

Sonal N. Mehta
Wilmer Cutler Pickering Hale and Dorr LLP
2600 El Camino Real, Suite 400
Palo Alto, CA 94306
Tel: (650) 858-6000
Email: sonal.mehta@wilmerhale.com

David Z. Gringer
Wilmer Cutler Pickering Hale and Dorr LLP
7 World Trade Center
250 Greenwich Street
New York, NY 10007
Tel: (212) 230-8800
Email: david.gringer@wilmerhale.com

**4. SPECIFICATION OF THE DATE BY WHICH THE REQUESTING AUTHORITY
REQUIRES RECEIPT OF THE RESPONSE TO THE LETTER OF REQUEST:**

1 The Requesting Authority would greatly appreciate a response to the Request for
2 Assistance as soon as is practicable, to ensure that the documents are received in a timely manner
3 for use in the civil proceedings described below.

4 **SECTION II**

5 **IN CONFORMITY WITH ARTICLE 3 OF THE CONVENTION, THE UNDERSIGNED**
6 **APPLICANT HAS THE HONOR TO SUBMIT THE FOLLOWING INFORMATION**
7 **REGARDING THE INSTANT REQUEST:**

8 **5. (a) REQUESTING JUDICIAL AUTHORITY (Article 3(a)):**

9 The Honorable James Donato
10 United States District Court of the Northern District of California
11 450 Golden Gate Avenue
12 San Francisco, CA 94102
13 United States of America

14 **(b) TO THE COMPETENT AUTHORITY OF (Article 3(a)):**

15 The British Virgin Islands

16 **(c) NAME OF THE CASE AND ANY IDENTIFYING NUMBER:**

17 *Klein, et al. v. Meta Platforms, Inc.*, No. 3:20-cv-08570-JD, United States District Court
18 for the Northern District of California, San Francisco, CA, U.S.A.

19 **6. NAMES AND ADDRESSES OF THE PARTIES AND THEIR**
20 **REPRESENTATIVES (Article 3(b)):**

21 **(a) Plaintiffs:**

22 Maximilian Klein

23 Sarah Grabert

24 Rachel Banks Kupcho

25 Affilious, Inc.

26 Jessyca Frederick

27 Mark Young

1 406 Property Services, PLLC

2 Mark Berney

3 Katherine Looper

4
5 Representatives:

6 Stephen A. Swedlow
7 Quinn Emanuel Urquhart & Sullivan, LLP
8 191 N. Wacker Drive, Suite 2700
9 Chicago, IL 60606
Tel: (312) 705-7400
Email: stephenswedlow@quinnemanuel.com

10 Shana E. Scarlett
11 Hagens Berman Sobol Shapiro LLP
12 715 Hearst Avenue, Suite 202
13 Berkeley, CA 94710
Tel: (510) 725-3000
Email: shanas@hbsslaw.com

14 Yavar Bathaee
15 Bathaee Dunne LLP
16 445 Park Avenue, 9th Floor
17 New York, NY 10022
Tel: (332)322-8835
Email: yavar@bathaeedunne.com

18 Kristen M. Anderson
19 Scott+Scott Attorneys at Law LLP
20 230 Park Avenue, 17th Floor
21 New York, NY 10169
Tel: (212) 223-6444
Email: kanderson@scott-scott.com

22 **(b) Defendant:**

23 Meta Platforms, Inc.
24 1601 Willow Road
Menlo Park, CA 94025

25 Representatives:

26 Sonal Mehta
27 Wilmer Cutler Pickering Hale and Dorr LLP
28 2600 El Camino Real, Suite 400
Palo Alto, CA 94306

1 Tel: (650) 858-6000
 Email: sonal.mehta@wilmerhale.com

2 David Z. Gringer
 3 Wilmer Cutler Pickering Hale and Dorr LLP
 4 7 World Trade Center
 5 250 Greenwich Street
 New York, NY 10007
 6 Tel: (212) 230-8800
 Email: david.gringer@wilmerhale.com

7 **7. NATURE AND PURPOSE OF THE PROCEEDINGS AND SUMMARY OF THE**
 8 **FACTS (Article 3(c)):**

9 **(a) Nature of the proceedings:**

10 The nature of the proceeding is a consolidated civil action brought on behalf of two putative
 11 classes: (1) a putative Consumer Class (consisting of individuals who use Meta's social networking
 12 and social media services); and (2) a putative Advertiser Class (consisting of individuals and
 13 entities that purchased Meta's advertising services). Consumer Plaintiffs bring claims under
 14 Section 2 of the Sherman Act alleging that Meta obtained and maintains monopoly power in the
 15 purported Social Network and Social Media Markets through allegedly false representations about
 16 its data collection and use practices. Advertiser Plaintiffs bring claims under Sections 1 and 2 of
 17 the Sherman Act for Meta's alleged monopolization and attempted monopolization of the
 18 purported Social Advertising market, including an alleged market division agreement between
 19 Meta and Google. These claims are based on the Consumer Plaintiffs' Consolidated Class Action
 20 Complaint, Dkt. No. 87, and the Advertiser Plaintiffs' First Amended Consolidated Class Action
 21 Complaint, Dkt. No. 237.

22 **(b) Summary of complaint:**

23 Consumer Plaintiffs: Consumer Plaintiffs allege that Meta has engaged in deceptive
 24 practices regarding the data privacy protections it provides to users of its services. Consumer
 25 Plaintiffs claim that Meta falsely represented that it would provide users with certain privacy
 26 protections and deceived users about the amount of user data that it harvested and made available
 27 to third parties. Consumer Plaintiffs allege that Meta's misrepresentations caused many users to use
 28 Meta's services over other competing platforms, which allowed Meta to obtain and maintain a

monopoly position in the “social network” and “social media” markets. A copy of the Consumer Plaintiffs’ Consolidated Class Action Complaint is attached as Attachment A.

Advertiser Plaintiffs: Advertiser Plaintiffs similarly allege that Meta’s deceptive practices regarding its data privacy protections allowed Meta to acquire a monopoly position in the “social advertising” market. Advertiser Plaintiffs further allege that Meta engaged in anticompetitive practices to eliminate and prevent further competition. Specifically, Advertiser Plaintiffs claim that Meta prevented developers from building mobile applications that could become rival social networks and competitors in the social advertising market. Advertiser Plaintiffs also allege that Meta and Google entered an anticompetitive agreement in September 2018 that divided the online advertising market and helped Meta maintain its position in the social advertising market. A copy of the Advertiser Plaintiffs’ First Amended Consolidated Class Action Complaint is attached as Attachment B.

(c) Summary of defense:

For numerous reasons, Meta denies the allegations in the Consumer and Advertiser Plaintiffs’ complaints. This Letter of Request is intended to obtain information particularly relevant to the following defenses (which is not an exhaustive list of Meta’s defenses in this proceeding): The market, as defined by the Consumer and Advertiser Plaintiffs, is implausible; the industry and the public do not recognize the purported “social network,” “social media,” or “social advertising” markets; Meta does not have the requisite market share of the alleged markets; competition and consumers cannot be harmed from alleged monopolization of a market for a product distributed free to all users; Meta’s data privacy policies and practices are not a means to gain competitive advantage over other competitors; and Meta has always faced competition in any properly defined market.

SECTION III

8. EVIDENCE TO BE OBTAINED OR OTHER JUDICIAL ACT TO BE PERFORMED (Article 3(d)):

(a) Evidence to be obtained:

1 The assistance requested of the British Virgin Islands consists of obtaining copies of
2 documents in the possession of Telegram.

3 **(b) Purpose of the evidence sought:**

4 The evidence sought in this Letter of Request pertains to the allegations and defenses
5 described above and are to be used only in legal proceedings in the matter described. The evidence
6 is subject to a strict protective order as provided in Attachment C. The protective order ensures
7 that documents produced in this matter will not be used by Meta in any way other than for purposes
8 of the litigation. The protective order provides that a producing party such as Telegram may mark
9 its documents as Confidential or Highly Confidential; if it does, no one at Meta may see the
10 documents except two (in the case of Highly Confidential material) to four (in the case of
11 Confidential Material) in-house counsel who are not permitted to participate in Meta's competitive
12 decision-making for two years after receiving the documents.

13 The information sought in this Request is necessary in the interest of justice for Meta to
14 defend itself fairly against the allegations made by the Consumer and Advertiser Plaintiffs. In
15 particular, Telegram provides a popular and prominent cloud-based messaging service which users
16 view as a competitive substitute to Meta's products. In late 2021, when Meta's products
17 experienced a six-hour long outage, Telegram reportedly gained 70 million new users. The
18 evidence sought from Telegram regarding the market in which it operates, the share of that market,
19 and its competition with Meta products (such as Instagram and WhatsApp) for user time and
20 attention are relevant to Meta's defense, because the presence of other digital platform companies
21 such as Telegram demonstrates that Meta lacks monopoly power in any market.

22 Meta seeks discovery from Telegram to show that Telegram has competed with Meta's
23 products. Meta seeks documents related to how Telegram views competition between Telegram
24 and Meta (Document Request No. 1) and whether Telegram's services provide users with features
25 substantially similar to those provided by Meta (Document Request No. 2). Meta also asks
26 whether Telegram has considered compensating its users for data to test Plaintiffs' damages theory
27 (Document Request No. 3). To address Plaintiffs' allegations related to market power, Meta is
28

requesting documents related to whether Telegram believes that its privacy policies and practices differentiate its products from those offered by its competitors or impact user satisfaction or engagement (Document Request No. 4 & 5). Lastly, Meta has two limited data requests related to Plaintiffs' allegations of market share and market definition regarding time spent on Telegram and the number of Daily Active Users (Document Request Nos. 6 & 7). Meta believes that this information is relevant to countering Plaintiffs' allegations that Meta has monopoly power in any cognizable market. Meta limited these requests to time spent, active users, and daily active users, which have been recognized as "appropriate indicators" of "market share." *See Fed. Trade Comm'n v. Facebook, Inc.*, 2022 WL 103308, at *7 (D.D.C. Jan. 11, 2022). Request Number 6 seeks data limited to specific periods of time when there was an outage on Meta's products and seeks information related to diversion from Meta's products. In Request Number 7, Meta has asked for data from 2013-2016 and 2021 to help respond to Plaintiffs' allegations that Meta has any type of durable monopoly power.

9. DOCUMENTS OR OTHER PROPERTY TO BE INSPECTED (Article 3(g)):

Attached as Attachment D is a list of documents to be obtained from Telegram.

10. SPECIAL METHODS OR PROCEDURES TO BE FOLLOWED (Article 3(i) & 9):

To the extent permitted by applicable laws, it is respectfully requested that the appropriate judicial authority of the British Virgin Islands require that the requested documents be duly marked for identification and produced in electronic and/or paper format, bearing such identification, to:

David Z. Gringer
 Wilmer Cutler Pickering Hale and Dorr LLP
 7 World Trade Center
 250 Greenwich Street
 New York, NY 10007
 Tel: (212) 230-8800
 Email: david.gringer@wilmerhale.com

It is further requested that, if permitted under the laws of the British Virgin Islands, the document production be accompanied by a sworn statement from an authorized Telegram agent, which attests to the fact that the production comprises the entirety of the documents described herein, or otherwise specifies what documents have been omitted and the reasons for their

omission, and which authenticates the documents as true and accurate copies of the documents described herein.

11. REQUEST FOR NOTIFICATION OF THE TIME AND PLACE FOR THE EXECUTION OF THE REQUEST AND IDENTITY AND ADDRESS OF ANY PERSON TO BE NOTIFIED (Article 7):

It is requested that notice of the execution of the Request be provided to the parties' representatives listed in paragraph 6 above.

12. REQUEST FOR ATTENDANCE OR PARTICIPATION OF JUDICIAL PERSONNEL OF THE REQUESTING AUTHORITY AT THE EXECUTION OF THE LETTER OF REQUEST (Article 8):

None.

13. AUTHORITY APPOINTING COMMISSIONER, PENDING APPROVAL OF THE MINISTRY OF JUSTICE:

The United States District Court for the Northern District of California.

14. SPECIFICATION OF PRIVILEGE OR DUTY TO REFUSE TO GIVE EVIDENCE UNDER THE LAW OF THE STATE OF ORIGIN (Article 11(b)):

In addition to the privileges applicable under BVI laws, Telegram need not disclose documents and electronic records which constitute confidential communications between it and its attorneys to the extent those communications seek or provide legal advice. This privilege may be waived, however, if the communication has been disclosed to third parties.

15. THE FEES AND COSTS INCURRED WHICH ARE REIMBURSABLE UNDER THE SECOND PARAGRAPH OF ARTICLE 14 OR UNDER ARTICLE 26 OF THE CONVENTION WILL BE BORNE BY:

The costs of this Hague Evidence Convention process, including the fees of the Commissioner, will be borne by Meta Platforms, Inc., c/o its counsel as identified above. Each party will be responsible for the fees and expenses, if any, of its own attorneys relating to any proceedings arising from this Hague Evidence Convention process.

SECTION IV

This District Court expresses its gratitude to the authorities of the British Virgin Islands for their assistance and courtesy under the terms of the Hague Convention.

Signature and Seal of the Requesting Authority:

Dated:

JAMES DONATO
UNITED STATES DISTRICT JUDGE

ATTACHMENT A

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

QUINN EMANUEL URQUHART & SULLIVAN, LLP
Stephen A. Swedlow (admitted *pro hac vice*)
stephenswedlow@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
(312) 705-7400

HAGENS BERMAN SOBOL SHAPIRO LLP
Shana E. Scarlett (Bar No. 217895)
shanas@hbsslw.com
715 Hearst Avenue, Suite 202
Berkeley, CA 94710
(510) 725-3000

Interim Co-Lead Consumer Class Counsel

[Additional counsel listed on signature page]

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION**

MAXIMILIAN KLEIN, SARAH GRABERT,
and RACHEL BANKS KUPCHO, on behalf of
themselves and all others similarly situated,

Plaintiffs,

vs.

FACEBOOK, INC.,

Defendant.

This Document Relates To: All Actions

Consolidated Case No. 5:20-cv-08570-LHK

The Hon. Lucy H. Koh

**CONSOLIDATED CONSUMER CLASS
ACTION COMPLAINT**

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

| | <u>Page</u> |
|--|-------------|
| I. PRELIMINARY STATEMENT..... | 1 |
| II. PARTIES | 5 |
| A. Defendant | 5 |
| B. Plaintiffs | 6 |
| III. JURISDICTION, VENUE, INTRADISTRICT ASSIGNMENT, AND CHOICE OF LAW | 8 |
| IV. FACTUAL ALLEGATIONS..... | 9 |
| A. General Background on the Social Media Industry | 9 |
| B. General Background on Facebook | 11 |
| C. Facebook is Dominant in the Social Network and Social Media Relevant Markets..... | 15 |
| 1) The Social Network Market | 15 |
| 2) The Social Media Market..... | 22 |
| 3) Relevant Geographic Market | 25 |
| 4) The Social Network and Social Media Markets Feature High Entry Barriers..... | 25 |
| D. Facebook Has Attempted to Acquire Market Power (and Has Succeeded in Acquiring Market Power) by Deceiving Consumers about Its Privacy Practices. | 31 |
| E. The Cambridge Analytica Scandal Partially Reveals the Extent of Facebook’s Deception. | 42 |
| F. Facebook Uses Anticompetitive Acquisitions and Threats to Destroy Competition in the Social Network and Social Media Markets..... | 47 |
| 1) Facebook’s Tracking of Consumers Drove Its Copy, Acquire, or Kill Strategy. | 47 |
| 2) Facebook Threatened Competitors with Discriminatory Practices to Help Drive its Anticompetitive Acquisition Strategy. | 51 |
| Instagram..... | 56 |
| Snapchat | 59 |
| WhatsApp..... | 61 |
| Other Examples of Facebook’s “Copy, Acquire, Kill” Strategy | 62 |

| | | | |
|----|-------|--|----|
| 1 | G. | Facebook’s Use of Onavo Comes to Light. | 63 |
| 2 | H. | Facebook’s Anticompetitive Practices Have Harmed and Continue to Harm Competition in the Social Network and Social Media Markets..... | 65 |
| 3 | I. | Facebook’s Anticompetitive Conduct Has Directly and Quantifiably Damaged Consumers. | 67 |
| 4 | | | |
| 5 | V. | STATUTE OF LIMITATIONS | 71 |
| 6 | A. | Accrual of Claim..... | 71 |
| 7 | B. | Equitable Tolling..... | 72 |
| 8 | C. | Fraudulent Concealment | 73 |
| 9 | D. | Continuing Violations and Ascertainment of Damages..... | 78 |
| 10 | VI. | CLASS ACTION ALLEGATIONS | 78 |
| 11 | VII. | INTERSTATE TRADE AND COMMERCE..... | 81 |
| 12 | VIII. | CLAIMS FOR RELIEF | 82 |
| 13 | IX. | PRAYER FOR RELIEF..... | 90 |
| 14 | X. | DEMAND FOR JURY TRIAL..... | 91 |
| 15 | | | |
| 16 | | | |
| 17 | | | |
| 18 | | | |
| 19 | | | |
| 20 | | | |
| 21 | | | |
| 22 | | | |
| 23 | | | |
| 24 | | | |
| 25 | | | |
| 26 | | | |
| 27 | | | |
| 28 | | | |

1 1. Plaintiffs, by their undersigned counsel, hereby bring this action against Defendant
2 Facebook, Inc. (“Facebook”), individually and on behalf of a Class of similarly situated persons,
3 and allege as follows:

4 **I. PRELIMINARY STATEMENT**

5 2. Founded originally as a website that allowed college students to connect with friends
6 on campus, Facebook has since expanded exponentially and today is both the largest social network
7 and the largest social media company in the world. In July 2020, for example, Facebook reported
8 1.78 billion daily active users and 2.7 billion monthly active users for its Facebook social network
9 alone. Including *all* of Facebook’s primary product offerings—*e.g.*, Facebook, Instagram,
10 Facebook Messenger, WhatsApp, and Oculus—Facebook commands 2.47 billion daily active users
11 and 3.14 billion monthly active users. But Facebook did not, as it would have the public believe,
12 obtain market dominance based on innovation and fair competition. Instead, Facebook has used its
13 behemoth-status as a weapon to clear the field of any and all competitors that threaten to take away
14 market share. Facebook has done so by engaging in a two-part anticompetitive scheme that
15 originated many years ago but continues to this day, and which has the net effect of destroying
16 competition and harming consumers.

17 3. First, set on utter domination, Facebook consistently and intentionally deceived
18 consumers about the data protections it provided to its users, in order to diminish competition and
19 obtain dominance in markets characterized by strong network effects and high barriers to entry.
20 During the early days of social networks, Facebook recognized that promising users stringent
21 privacy protections was necessary for it to win the race for market adoption. Accordingly, many
22 users chose Facebook over other competing networks due to Facebook’s stated commitment to its
23 users’ privacy. In reality, however, Facebook concealed the scope of the data it harvested from
24 consumers and the ways in which it used that data to squash competition. By the time Facebook’s
25 deception began to come to light in 2018, it was too late—Facebook had cheated its way to market
26 dominance. Facebook’s deceptions allowed the company to gain and then, over the years, illegally
27 maintain a stranglehold on the Social Network and Social Media Markets (defined and discussed
28 further below). And high barriers to entry, including strong network effects and high switching

costs, bolstered Facebook’s efforts to prevent actual and would-be competitors alike from challenging its monopolistic grip.

4. Second, Facebook exploited the rich data it deceptively extracted from its users to identify nascent competitors and then “acquire, copy, or kill” these firms. Rather than competing on the merits, Facebook used the valuable consumer data that it was harvesting to identify incipient competitors with the most likely path to meaningful market share gains. Equipped with the valuable user data it led consumers to believe it was not gathering and would not use in this way, Facebook targeted its users’ preferred alternatives for destruction. Facebook made clear that it would copy incipient competitors’ innovations and discriminatorily shut off these firms’ access to Facebook’s valuable user data if they did not sell their businesses to Facebook first. The message to its competitors was explicit: sell at a bargain, or Facebook will go into “destroy mode.” All of this was enabled by Facebook’s deception.

5. While Facebook’s scheme—bolstered by its deception and its serial acquisitions—has allowed Facebook to evolve since Mark Zuckerberg founded the company in 2004, the basic economic relationship between Facebook and its users has not. When users sign up for a Facebook account, they agree to certain terms. Those terms lay out the economic exchange between Facebook and its users. Consumers give Facebook access to, and use of, certain types and amounts of personal data about themselves; Facebook allows users to access its social network and social media offerings and pledges to protect users’ privacy. Facebook’s current Terms of Service state:

Instead of paying to use Facebook and the other products and services we offer, by using the Facebook Products covered by these Terms, you agree that we can show you ads that businesses and organizations pay us to promote on and off the Facebook Company Products. We use your personal data, such as information about your activity and interests, to show you ads that are more relevant to you.¹

Notably, Facebook suggests to users (even to this day) that the extent to which it utilizes their data is limited, and that the extent of the data collection is limited to Facebook’s services themselves.

6. The Terms of Service further state that “[i]n exchange [for access to Facebook’s services] we need you to make [certain] commitments.” Among those “commitments” is

¹ *Facebook Terms of Service*, <https://www.facebook.com/terms.php> (last accessed Apr. 15, 2021) (emphases added).

1 “[p]ermission to use your name, profile picture, and information about your actions with ads and
 2 sponsored content.” The Terms then state that protecting user “privacy is central to how [Facebook
 3 has] designed [its] ad system.” In other words, consumers give up personal information and agree
 4 to receive targeted advertisements on Facebook in exchange for access to Facebook’s social
 5 network. Consumers do not agree to anything beyond that.

6 7. Facebook derives enormous economic value from the data it harvests from
 7 consumers. In fact, Facebook itself touts the economic value of the data it harvests from consumers.
 8 Facebook sells ads targeted to users based on the personal data that it collects from them. And,
 9 Facebook specifically describes its massive advertising earnings in terms of average revenue per
 10 user (“ARPU”) in its public filings. For 2019, Facebook reported that its ARPU was over \$41.00
 11 per user in the United States and Canada.² At over 200 million users in the United States, that
 12 amounts to over \$8.2 billion in revenue that Facebook derived in a single year.

13 8. Facebook’s weaponization of user data and its strategy to “acquire, copy, or kill”
 14 competitors has been wildly successful at the expense of consumers. Facebook’s anticompetitive
 15 scheme has lessened, if not eliminated, competition and harmed consumers.

16 9. Facebook’s destruction of competition has caused consumers to suffer substantial
 17 economic injury. Consumers give up something of material value when agreeing to use Facebook’s
 18 products: their personal data and their attention. As Facebook’s co-founder explained, “[Facebook]
 19 is not actually free, and it certainly isn’t harmless. . . . We pay for Facebook with our data and our
 20 attention, and by either measure it doesn’t come cheap.”³ User data and attention is then sold in
 21 measurable units to advertisers in exchange for money.

22 10. Absent Facebook’s anticompetitive scheme, fair competition would have required
 23 Facebook to provide consumers greater value in return for consumers’ data on a market-wide basis,
 24 but Facebook instead took that data without providing adequate consideration to its users (*i.e.*, the
 25 members of the putative class in this action). That constitutes antitrust injury. Through its

26 ² Facebook Q4 2019 Results at 4, available at <https://kl.link/36yIY5J> (last accessed Apr. 15,
 27 2021).

28 ³ Chris Hughes, *It’s Time to Break Up Facebook*, The New York Times (May 9, 2019),
 available at <https://kl.link/3dUTshC> (last accessed Apr. 15, 2021).

1 deception and the acquisitions enabled by its deception, Facebook prevented competition on the
 2 merits, and as a result of that reduction in competition, users received less value for their data than
 3 they would have received absent the reduction.

4 11. Facebook's acquisition and maintenance of monopoly power continues to harm
 5 consumers. Prior to Facebook's consolidation of the Social Network and Social Media Markets, a
 6 number of firms vigorously competed to win over consumers by offering competing products which
 7 differed in non-price attributes such as quality. For instance, early social networks and social media
 8 companies, including Facebook, competed for market share by offering competing products to
 9 consumers which highlighted particular privacy features. Absent Facebook's anticompetitive
 10 scheme, which has allowed Facebook to place consumers under its monopolistic thumb,
 11 competition from Facebook's rivals would require Facebook to give consumers greater value in
 12 exchange for their use of Facebook, through monetary consideration or higher quality offerings.
 13 Instead, Facebook's anticompetitive conduct has allowed Facebook to artificially stifle innovation
 14 and deprive consumers of any meaningful alternative to Facebook's social network and social
 15 media empire. As a result, consumers are faced with a "take it or leave it choice": accept a
 16 Facebook of lesser value and quality or forgo use of the only social network and social media
 17 offerings used by most consumers' friends and family members.

18 12. Facebook's monopolistic conduct violates the antitrust laws and harms consumers.
 19 Indeed, the United States House of Representatives Antitrust Subcommittee, the Federal Trade
 20 Commission ("FTC"), and various State Attorneys General have all recognized that Facebook has
 21 engaged in anticompetitive conduct. A recent majority staff report from the House Antitrust
 22 Subcommittee details Facebook's pattern of anticompetitive conduct. *See Investigation of*
 23 *Competition in Digital Markets*, Majority Staff Report and Recommendations ("House Report"),
 24 Subcommittee on Antitrust, Commercial, and Administrative Law of the Committee on the
 25 Judiciary (Oct. 6, 2020), available at <https://kl.link/3jGISfK>. And, the FTC and 48 State Attorneys
 26 General have commenced civil antitrust lawsuits against Facebook. *See State of New York et al v.*
 27 *Facebook, Inc.*, Case No. 1:20-cv-03589-JEB (D.D.C.); *Federal Trade Commission v. Facebook,*
 28 *Inc.*, Case No. 1:20-cv-03590-JEB (D.D.C.).

13. Facebook is dominant in the Social Network Market and the Social Media Market, and it has engaged in predatory and exclusionary conduct in order to monopolize those markets, causing Plaintiffs and Consumer Class members to suffer substantial economic injury. This action seeks recovery for consumers' losses and Facebook's unlawful gains and appropriate equitable relief to prevent Facebook from continuing to destroy competition and harm consumers.

II. PARTIES

A. Defendant

14. Founded by Mark Zuckerberg in 2004, Defendant Facebook, Inc. is a Delaware corporation with its principal place of business located in Menlo Park, California.

15. Facebook is a social media company that provides online services to more than 3.14 billion users. Facebook owns and operates several business divisions, such as:

- Facebook. Facebook's core social networking application, which bears the company's name, is, according to Facebook's filings with shareholders, designed to enable "people to connect, share, discover, and communicate with each other on mobile devices and personal computers." The Facebook core product contains a "News Feed" that displays an algorithmically ranked series of content, including a wide range of media and updates regarding the activities of the user's social connections. The News Feed also includes advertisements individualized for each person.
- Instagram. Instagram is a social media photo-sharing application that allows users to share photos, videos, and messages on mobile devices. Facebook announced that it was acquiring Instagram in April 2012, consummating the acquisition later that year.
- Messenger. Facebook's Messenger application is a multimedia messaging application, allowing messages that include photos and videos to be sent from person to person across applications and devices.
- WhatsApp. WhatsApp is a messaging application used by individuals and businesses. One of WhatsApp's primary selling points is the claim that it is more

1 private and secure than text messages or other messaging apps. Facebook acquired
2 WhatsApp in 2014.

3 16. In exchange for providing services, Facebook collects user data, which it allows
4 advertisers to use for targeted advertising to Facebook users. Facebook's principal revenue is from
5 targeted advertising that it provides to advertisers. In 2019, Facebook collected \$70.7 billion in
6 revenue, almost entirely from allowing companies to serve ads to its users.

7 17. Facebook has over 50,000 employees and offices worldwide.

8 **B. Plaintiffs**

9 18. Plaintiff Maximilian Klein is a natural person and citizen of the State of Vermont
10 and a resident of Chittenden County.

11 19. Plaintiff Klein created a Facebook account in 2006, maintains an active account, and
12 regularly uses Facebook. Plaintiff Klein has an active Instagram account and has maintained that
13 account since 2016. Plaintiff Klein uses Facebook's Messenger feature and actively uses a
14 WhatsApp account.

15 20. Plaintiff Klein cares about his online privacy and trusted Facebook to protect his
16 privacy. But since the Cambridge Analytica scandal broke in 2018 and exposed Facebook's lack
17 of privacy protections and low-quality data privacy practices, he now does not trust Facebook to
18 protect his online privacy. Plaintiff Klein now does not like the invasiveness of Facebook and its
19 products. Despite this, Plaintiff Klein continues to use Facebook and its products because virtually
20 everyone he knows uses them and there are no other suitable alternatives to connect with his friends
21 and family.

22 21. Facebook lied about its data privacy practices and the scope of the data it collected
23 and made available to third parties. If Plaintiff Klein had known the truth about Facebook's privacy
24 practices years ago, he would not have agreed to give Facebook access to as much personal data
25 about himself.

26 22. Plaintiff Sarah Grabert is a natural person and citizen of the State of Illinois and a
27 resident of Cook County.
28

23. Plaintiff Grabert created a Facebook account prior to 2007, maintains an active account, and regularly uses Facebook. Plaintiff Grabert has an active Instagram account and has maintained that account since at least 2010. Plaintiff Grabert uses Facebook's Messenger feature and has used a WhatsApp account.

24. Plaintiff Grabert cares about her online privacy and trusted Facebook to protect her privacy. But since the Cambridge Analytica scandal broke in 2018 and exposed Facebook's lack of privacy protections and low-quality data privacy practices, she now does not trust Facebook to protect her online privacy. Plaintiff Grabert now does not like the invasiveness of Facebook and its products. Despite this, Plaintiff Grabert continues to use Facebook and its products because virtually everyone she knows uses them and there are no other suitable alternatives to connect with her friends and family.

25. Facebook lied about its data privacy practices and the scope of the data it collected and made available to third parties. If Plaintiff Grabert had known the truth about Facebook's privacy practices years ago, she would not have agreed to give Facebook to as much personal data about herself.

26. Plaintiff Rachel Banks Kupcho is a natural person and citizen of the State of Minnesota and a resident of Hennepin County. Plaintiff Banks Kupcho created a Facebook account in approximately 2008, maintains an active account, and regularly uses Facebook. Plaintiff Banks Kupcho actively uses her Instagram account, Facebook's Messenger feature, and her WhatsApp account.

27. Plaintiff Banks Kupcho cares about her online privacy and trusted Facebook to protect her privacy. But since the Cambridge Analytica scandal broke in 2018 and exposed Facebook's lack of privacy protections and low-quality data privacy practices, she now does not trust Facebook to protect her online privacy. Plaintiff Banks Kupcho now does not like the invasiveness of Facebook and its products. Despite this, Plaintiff Banks Kupcho continues to use Facebook and its products because virtually everyone she knows uses them and there are no other suitable alternatives to connect with her friends and family.

28. Facebook lied about its data privacy practices and the scope of the data it collected and made available to third parties. If Plaintiff Banks Kupcho had known the truth about Facebook's privacy practices years ago, she would not have agreed to give Facebook to as much personal data about herself.

III. JURISDICTION, VENUE, INTRADISTRICT ASSIGNMENT, AND CHOICE OF LAW

29. This action arises under Section 2 of the Sherman Antitrust Act, 15 U.S.C. § 2, and Section 4 of the Clayton Act, 15 U.S.C. § 15. The action seeks to recover treble damages or disgorgement of profits, interest, costs of suit, equitable relief, and reasonable attorneys' fees for damages to Plaintiffs and members of the Consumer Class resulting from Facebook's restraints of trade and monopolization of the Social Network and Social Media Markets described herein.

30. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 (federal question), 28 U.S.C. § 1332 (class action diversity jurisdiction), 28 U.S.C. § 1337(a) (antitrust), and 15 U.S.C. § 15 (antitrust). The Court also has subject matter jurisdiction over the state-law unjust enrichment claims presented in this action under 28 U.S.C. 1367 (supplemental jurisdiction).

31. This Court has personal jurisdiction over Facebook because it is subject to general jurisdiction in the State of California, where it maintains its headquarters and its principal place of business, and Facebook's Terms provide that consumers must bring these claims in this Court. The scheme to monopolize alleged in this Complaint caused injury to persons throughout the United States, including in this District. Moreover, Facebook also conducted substantial business from which the claims in this case arise in California and has agreed to personal jurisdiction in this Court.

32. Venue is appropriate in this District under 15 U.S.C. § 15(a) (Clayton Act), 15 U.S.C. § 22 (nationwide venue for antitrust matters), and 28 U.S.C. § 1391(b) (general venue provision). Facebook transacts business within this District, and it transacts its affairs and carries out interstate trade and commerce, in substantial part, in this District.

33. This action is properly assigned to the San Jose Division of this District, pursuant to Civil Local Rule 3-2(c), because antitrust class actions may be assigned on a district-wide basis.

34. To the extent there is a choice of law, Facebook’s “Terms of Service” provide that “the laws of the State of California” govern “any claim” between Facebook and its users that “arises out of or relates to “the Facebook Products[.]”⁴

IV. FACTUAL ALLEGATIONS

A. **General Background on the Social Media Industry**

35. At a high level, the various participants in the social media industry include the following: social media applications, social networks, consumers, advertisers, and content providers (which can be any of the previous types of market participants, or can be third parties).

36. Social media applications provide limited access to user-generated content—such as text posts or comments, digital photos or videos, and data generated through online interactions. Indeed, social media applications often focus, at least initially, on a particular form of media.⁵ Twitter, for example, developed as an application for broadcasting users’ short text messages (originally limited to 140 characters, and which now allows for up to 280 characters). YouTube facilitates the sharing of videos of varying temporal length, while TikTok allows for the sharing of short-form videos of limited temporal length. Instagram distinguishes itself as an application for the sharing of photos and, to a lesser extent, videos.

37. A social *network*, on the other hand, is distinct from a social media application. While social media applications often facilitate the sharing of a distinct form of content—*i.e.*, photographs (Instagram), short text messages (Twitter), disappearing messages (Snapchat), or short-form videos (TikTok)—social networks (such as Facebook, and, previously, Myspace, Friendster, Orkut, Flip.com, Bebo, and Google+) combine these and other individual features and allow their users to access them as part of one, multi-function product. In addition, social networks typically allow users on their networks to connect and interact with a full spectrum of the users’

⁴ Facebook Terms of Service, <https://www.facebook.com/terms.php> (last accessed Apr. 15, 2021).

⁵ House Report, *supra*, at 89–90 (“Social media companies may also focus on attracting particular types or groups of consumers to differentiate themselves from larger companies. . . . Given Facebook’s dominance, the primary way for new entrants to compete is to attract a subgroup or niche.”).

social connections (including people the users already know), participate in “groups” which join together users with a particular background or common interest, and display content through linear feeds.⁶ Facebook’s social network—which allows users to interact with others, join and participate in groups, and display a wide variety of content linearly—is pictured below.⁷



38. Social networks and social media applications typically offer their services to consumers for non-cash consideration.⁸ In consideration for providing services, social networks and social media applications obtain valuable personal data from their users. The extent of the information obtained from users varies by social network and by social media application, as do the disclosures about what data is obtained and the uses to which it is subsequently put.

39. Social networks and social media applications monetize the data they obtain from users by selling access to the data to third parties. As the FTC’s former Chief Technologist has explained with respect to Facebook in particular, “personal information . . . is given to the platform,

⁶ House Report, *supra*, at 88.

⁷ See Kessica Guynn, *Facebook is making a big change to your news feed*, USA TODAY (Jan. 11, 2018), available at <https://www.usatoday.com/story/tech/2018/01/11/facebook-newsfeed-big-change/1023331001/> (last accessed Apr. 15, 2021).

⁸ House Report, *supra*, at 88.

1 mined, and then resold to or reused by third-party developers to develop apps, or resold to
 2 advertisers to advertise with.”⁹ To illustrate, advertisers, product manufacturers, and service
 3 providers often pay social networks and social media applications to direct curated ads specifically
 4 towards particular user segments.

5 **B. General Background on Facebook**

6 40. Facebook’s core offering to consumers is access to its social network, which
 7 contains the individualized profiles of well over 200 million users in the United States and billions
 8 of users worldwide and integrates with it Facebook’s various social media offerings. In exchange
 9 for access to the only social network that allows consumers to connect online with most of their
 10 family, friends, and acquaintances, Facebook requires users to provide their personal data and
 11 receive targeted advertisements.

12 41. Facebook uses the data obtained from its massive user base to generate its largest
 13 source of income: selling targeted advertisements to its users. Indeed, Facebook publicly
 14 acknowledges that “[w]e generate substantially all of our revenue from advertising.”¹⁰ In 2019,
 15 Facebook collected \$70.7 billion in revenue, almost entirely from allowing companies to serve
 16 targeted ads to its users.

17 42. Facebook’s machine learning algorithms mine patterns in the data for advertisers,
 18 which allows advertisers to reach precisely the right audience to convert into sales, user signups,
 19 or the generation of sales leads. To protect its control over user data, Facebook has brought legal
 20 action against actors that have copied publicly available user data and made it available outside of
 21 Facebook, demonstrating that Facebook recognizes the value of this data.¹¹

22 ⁹ United Kingdom House of Commons, Digital, Culture, Media and Sport Committee,
 23 *Disinformation and ‘Fake News’: Final Report*, 2017-19, HC 1791, (“DCMS Report”) (Feb. 14,
 24 2019), at ¶ 128, available at <https://kl.link/37MnyDf> (last accessed Apr. 15, 2021). Indeed, as the
 25 U.K. House of Common’s Digital, Culture, Media and Sport Committee has recognized, “[i]n
 26 portraying itself as a free service, Facebook gives only half the story.” *Id.*

27 ¹⁰ Form 10-K Filing for Facebook, Inc., Securities and Exchange Commission, available at
 28 <https://www.sec.gov/Archives/edgar/data/1326801/000132680119000009/fb-12312018x10k.htm>
 at 42 (last accessed Apr. 18, 2021) (emphasis added).

¹¹ Facebook brought one such suit as recently as November 19, 2020. *See* Jessica Romero,
Combating Clone Sites, Facebook Newsroom (Nov. 19, 2020), available at
<https://about.fb.com/news/2020/11/combating-clone-sites/> (last accessed Apr. 15, 2021).

43. The data is also monetized by commercializing access—for example, by providing application developers, content generators, and advertisers with direct access to the information embedded in Facebook’s network, such as the interconnection between users, user attributes, and user behavior. That data can then be used by these third parties.

44. From the beginning, Facebook has sought to entice consumers based on its supposed commitment to maintaining the privacy of its users’ data. Unlike earlier competing social networks that allowed anyone interested to join anonymously or by using unverified usernames, Facebook required that those interested in joining use their real-world identities.

45. This qualitative distinction had clear privacy implications. Ironically, early applications that allowed users to register anonymously or with pseudonyms caused more privacy problems for users because wrongdoers that obtained and/or used fellow users’ personal information could hide behind their online (anonymous or unverified) identities.

46. In contrast, Facebook claimed that it created a level of accountability, because users ostensibly knew who was on the other side of the screen from them and were connected to them in some way in real life. Indeed, Facebook’s website “was one of the first social networks where users actually identified themselves using their real names.”¹² By making users “real,” Facebook claimed (and users agreed by voting with their feet) that their social interactions online were better protected and more meaningful. But all of this required Facebook to promise privacy protection in order to induce users to provide their real-world identities and data.

47. Mark Zuckerberg learned the importance of privacy to consumers early on. While a student at Harvard University, Mr. Zuckerberg created “Facemash,” which “juxtaposed the pictures of two random Harvard undergraduates and asked users to judge their physical attractiveness.”¹³ Facemash used the students’ photos without their permission, “dr[a]w[ing] the

¹² See John Gallagher, Getting the Most Out of Information Systems § 8.3, available at <https://kl.link/3dX3BKN> (last accessed Apr. 15, 2021).

¹³ Alan J. Tabak, *Hundreds Register for New Facebook Website*, The Harvard Crimson (Feb. 9, 2004), available at <https://www.thecrimson.com/article/2004/2/9/hundreds-register-for-new-facebook-website/> (last accessed Apr. 15, 2021).

ire of students and administrators alike[.]”¹⁴ While promoting “thefacebook.com,” Facebook’s predecessor, Zuckerberg vowed that he had learned from his experience with Facemash and would build into “thefacebook.com” “intensive privacy options,” which “he hoped would help to restore his reputation[.]”¹⁵ In reality, thefacebook.com’s—and later Facebook’s—representations regarding privacy were part of an orchestrated scheme, designed to secure and prolong monopoly status.

48. At first, Facebook was closed to all but those users who could validate their own real-world identities, such as by verifying that their identities were legitimate via an e-mail address issued by an organization, such as a university or a firm.¹⁶

It was this “realness” that became Facebook’s distinguishing feature—bringing along with it – and also depending on – a perceived degree of safety and comfort that enabled Facebook to become a true social utility and build out a solid social graph consisting of verified relationships. Since “friending” (which is a link between nodes in the social graph) required both users to approve the relationship, the network fostered an incredible amount of trust. Today, many Facebook users post their cell phone numbers and their birthdays, offer personal photos, and otherwise share information they’d never do outside their circle of friends.

49. The data Facebook has since collected derives much of its value from the ability to identify Facebook’s users by their real-world identities. Other applications, such as Twitter, have only loosely enforced identity rules, and have never required users to disclose granular details about themselves.

50. Facebook characterizes each user’s disclosure of his or her identity as increasing the value of the experience for all users, who are purportedly able to benefit from others’ disclosures by connecting with and following the activities of their real-world connections.¹⁷ Disclosure also

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ Gallaughier, *supra*, § 8.3.

¹⁷ Apple’s Senior Director for Global Privacy recently expressed skepticism that social networks and social media applications like Facebook encourage disclosure of personal information solely to create a richer “personalized experience” for other users. See Apple Privacy Letter, November 19, 2020, available at <https://kl.link/33bhK2Y> (last accessed Apr. 15, 2021) (“What some companies call ‘personalized experiences’ are often veiled attempts to gather as much data as possible about individuals, build extensive profiles on them, and then monetize those profiles.”).

1 increases the market value of the data Facebook obtains from its users. Knowing the internet habits
 2 of “YankeesFan123” is less valuable than knowing the browsing habits of a specific individual
 3 whose love of the Yankees can be linked with data about his shopping habits, income, family,
 4 friends, travel, dining, dating, and myriad other data points.

5 51. In the years since its inception, Facebook has tracked trillions of data points about
 6 consumers with a powerful data structure it calls the “social graph.” The social graph “refers to
 7 Facebook’s ability to collect, express, and leverage the connections between the site’s users, or as
 8 some describe it, ‘the global mapping of everyone and how they’re related.’”¹⁸ All of the data on
 9 Facebook can be thought of as a “node” or “endpoint” that is connected to other data on Facebook:

10 You’re connected to other users (your friends), photos about you are tagged,
 11 comments you’ve posted carry your name, you’re a member of groups, you’re
 12 connected to applications you’ve installed—Facebook links them all.¹⁹

13 52. Given Facebook’s size and reach, as well as the extent of its surreptitious data
 14 collection, the social graph is a unique and uniquely valuable data set, even among the giants of the
 15 tech world. Much of this value stems from the fact that the majority of Facebook’s social graph
 16 cannot be viewed by the public or search engines and contains extraordinary amounts of data that
 17 users unwittingly provided Facebook regarding their most granular everyday habits.

18 53. Facebook is a so-called “walled garden”—a closed ecosystem run by a single
 19 operator. Advertisers must go through Facebook in order to reach Facebook users. And Facebook
 20 can decide how much of its social graph it allows advertisers and app developers, including
 21 competitors, to access.

22 54. The personal data of Facebook’s users takes many forms including data about the
 23 information users share on their personal profile pages, the photos and profiles users have viewed,
 24 what information users share with others, and even what users put in messages to other users. These
 25 granular data allow targeted advertising on a scale that has never before existed. Facebook’s

26 ¹⁸ Gallagher, *supra*, (quoting Alex Iskold, “Social Graph: Concepts and Issues,”
 27 ReadWriteWeb, September 12, 2007).

28 ¹⁹ *Id.* (citing Alan Zeichick, “How Facebook Works,” Technology Review, July/August
 2008).

products allow advertisers to target Facebook’s user base by their attributes and behavior. Third party advertisers have been able to use Facebook’s products to track and target consumers throughout the internet, even when Facebook users are “logged-out” of Facebook.

C. Facebook is Dominant in the Social Network and Social Media Relevant Markets.

55. There are two relevant markets applicable to this dispute. They are: (1) the Social Network Market; and (2) the Social Media Market. The House Antitrust Subcommittee has recognized both the Social Network Market and the Social Media Market as relevant markets.²⁰ Facebook has unlawfully acquired and maintained monopoly power in both markets.

1) The Social Network Market

56. The Social Network Market is the product market consisting of social networks, which are websites and applications that allow users to find, communicate, and interact with friends, family, personal acquaintances, and other people with whom the users have shared interests or connections. Examples of social networks include (among others) Facebook—and, while they existed—Myspace, Friendster, Orkut, Flip.com, Bebo, and Google+. A social network is distinct from a social media application, although a social media application may offer a limited part of the wide array of functions and connections of a social network. To that extent, as explained more fully below, the Social Network Market is a distinct part or sub-part of the Social Media Market.

57. Social networks feature several key elements which distinguish them from other services, including social media applications. First, social networks provide their users a “rich social experience” based on a social graph.²¹ A social graph connects users to a wide array of people, which is both extensive in number and vast in scope, reflecting the full range of connections that users have in the real world. This wide array includes people whom the users already know in real life (such as friends, family members, neighbors, community members, and other acquaintances), as well as people whom the users do not yet know, but whom are associated with the users’ other real-world acquaintances (such as a friend of a friend) or share some characteristic

²⁰ House Report, *supra*, at 90–91.

²¹ *Id.* at 91.

1 with the users (such as interests or background). Many social networks encourage their users to
 2 expand their networks by suggesting new people the users may connect to.

3 58. Second, social networks provide substantive features to users which facilitate a wide
 4 array of interaction among the wide array of people that make up a user's social graph, which
 5 reflects the full range of interactions that users have in the real world. To illustrate, social networks
 6 allow users to share content—including text posts, photos, videos, and other content matter—
 7 among their connections. And if, for instance, Sarah shares a picture with all of her connections
 8 on a social network, including with Tom and Jerry, a social network may allow Tom and Jerry to
 9 engage with each other through their shared connection to Sarah, even if Tom and Jerry do not
 10 already know each other. Social networks provide additional substantive features which facilitate
 11 users finding and engaging with each other, such as the ability to create and participate in groups,
 12 which bring together individuals with common backgrounds (such as graduates of a particular
 13 school), common interests (such as in a particular cuisine or in a specific film franchise), and
 14 common hobbies (such as restoring classic cars). As another example, social networks may also
 15 allow users to organize events among the wide array of people that make up the users' social graphs,
 16 including the abilities to create pages with information about an event, curate an invitation list, and
 17 send and monitor invitation lists. Some social networks even allow users to play online games with
 18 their connections.

19 59. Third, social networks provide users with the convenience of a “one-stop shop.”
 20 Social networks combine multiple substantive features and functionalities into one product, in a
 21 way that firms that may offer one individual feature do not. Mark Zuckerberg, Facebook's founder,
 22 has recognized the multi-functionality of Facebook as a distinct and important feature, explaining:
 23 “. . . there are so many different things that you can do. . . . Pretty much anything that you would
 24 want to do with a number of people at once, you can do in that digital equivalent of the town
 25 square.”²²

26
 27 ²² *Interview with Facebook CEO Mark Zuckerberg*, ABC News (Apr. 4, 2019), available at
 28 <https://abcnews.go.com/Business/interview-facebook-ceo-mark-zuckerberg-transcript/story?id=62152829> (last accessed Apr. 19, 2019).

60. There are no reasonable substitutes for social networks. Other applications either do not provide for social interaction with a network of people or provide only a single or limited part of the wide array of functions and connections of social networks. Search engines, such as Google, Yahoo, or Bing, are not “social networks” because they do not provide for interaction between application users. Similarly, apps like Apple’s “iMessage,” which simply allow the sharing of messaging media, such as emails or text messages, are not social networks because although they provide for interaction, they do so only in a device-to-device manner, among a limited number of the user’s contacts (such as those in the user’s address book), on a certain operating system, and focus solely on delivering messages rather than facilitating a broader online social experience.²³

61. Still other types of online networks, such as LinkedIn, are not “social networks,” as that term is defined in this complaint, because they are used for a different purpose, and are used in parallel to—rather than instead of—social networks. Whereas LinkedIn is typically considered the dominant professional online network in the world, it is not a replacement for social networks such as Facebook. This is because LinkedIn is used primarily by a narrow array of contacts for professional networking and employment-seeking purposes, while Facebook and its like are used primarily for non-professional, personal purposes.²⁴

62. Various governmental entities have recognized that LinkedIn is not a replacement for social networks, including Facebook.²⁵ During its review of the Microsoft/LinkedIn merger,

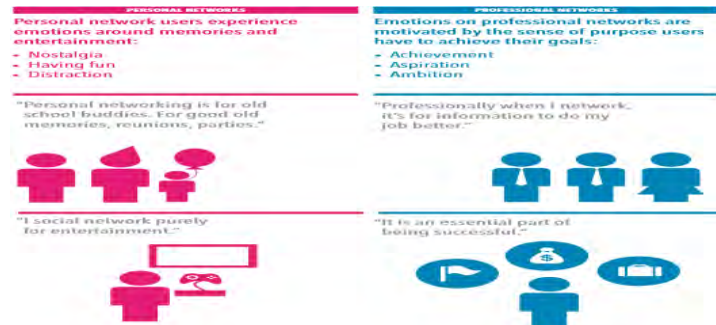
²³ Facebook itself has noted this distinction, explaining in documents provided to the House Antitrust Subcommittee that whereas the growth of Apple’s iMessage is “limited by the adoption of iPhones, . . . Facebook’s products can be used across devices.” *Id.* at 136 n.752.

²⁴ Facebook has, itself, recognized this distinction in documents it provided to the House Antitrust Subcommittee. *See id.* at 133–34 n.733 (“LinkedIn . . . coexist[s] in the US with similar user bases but orthogonal graphs: Facebook connects friends and family, LinkedIn connects coworkers[.]”).

²⁵ In their respective antitrust suits against Facebook, for example, the FTC and various State Attorneys General have all asserted that LinkedIn is not a substitute for social networks like Facebook. *State of New York et al v. Facebook, Inc.*, Case No. 1:20-cv-03589-JEB (D.D.C.), Dkt. 70, ¶ 34; *Federal Trade Commission v. Facebook, Inc.*, Case No. 1:20-cv-03590-JEB (D.D.C.), Dkt. 51, ¶ 58.

the European Commission explained: “the reasons for using a [professional service network] are different from those for using a personal social network. While the former is used to ‘1. Maintain professional identity, 2. Make useful contacts, 3. Search for opportunities, 4. Stay in touch’, the latter is used to ‘1. Socialize, 2. Stay in touch, 3. Be entertained, 4. Kill time’.”²⁶ Thus, users will have *both* a LinkedIn and a Facebook account, not one or the other, and this other type of network is not viewed or treated as a substitute for a social network.²⁷

63. LinkedIn itself has recognized social networks are a distinct product.²⁸ It has, for example, explained the differences between “personal networks” (e.g., Facebook) and “professional networks” (e.g., LinkedIn):²⁹



64. Similarly, LinkedIn has recognized the distinct content that social network users expect to see when visiting a given social network:³⁰

²⁶ European Commission, *Case M.8124 – Microsoft/LinkedIn* (June 12, 2016) at ¶ 106, available at https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf (last accessed Apr. 15, 2021) (emphases in original).

²⁷ In addition to recognizing LinkedIn’s distinct professional networking purpose, the House Antitrust Subcommittee’s recent report also distinguished LinkedIn from social networks, like Facebook, on the basis of LinkedIn’s economic model. Whereas users pay for social networks like Facebook with their data, time, and attention, some features of LinkedIn, such as “LinkedIn Premium,” further require users to pay a monetary fee. *See* House Report, *supra*, at 88.

²⁸ *See* LinkedIn, *The Mindset Divide* (Sept. 2012), available at https://business.linkedin.com/content/dam/business/marketing-solutions/global/en_US/site/pdf/wp/linkedin-marketing-solutions-mindset-divide.pdf (last accessed Apr. 15, 2021).

²⁹ *Id.* at 4.

³⁰ *Id.* at 6.



65. Social media applications, such as YouTube and TikTok, are likewise not reasonable substitutes for social networks. Indeed, the House Antitrust Subcommittee, Germany’s Federal Cartel Office, and the United Kingdom’s Competition and Markets Authority have all recognized the distinction between the Social Network Market and the Social Media Market and that “the specific demand for social networks is fundamentally different from the demand for other social media.”³¹ That is because users utilize each for different purposes: social networks “facilitate their users finding, interacting, and networking with other people they already know online,” whereas social media applications “principally facilitate the distribution and consumption of content” between “users with a wide range of relationships to the person posting, including by strangers.”³² Thus, while a user might use YouTube to access and watch a complete stranger’s video—such as a cooking recipe—the same user would use Facebook, not YouTube, to share *that* video with the user’s friends, family, and real-world connections.³³ Similarly, a user that finds a funny video of a celebrity (or other stranger) on YouTube may choose to encourage their friends and family to view that video by sharing it with them on Facebook with a note:³⁴

³¹ House Report, *supra*, at 91.

³² *Id.* at 91.

³³ See Administrative Proceedings, Bundeskartellamt, B6-22/16 (“German Federal Cartel Office Report”) ¶ 312 (Feb. 6, 2019), available at <https://kl.link/39AxErE> (last accessed Apr. 15, 2021) (“YouTube is hardly ever used for other purposes (e.g. contacts to friends, messaging, looking for people the user knows, share contents”).

³⁴ Meira Gebel, *How to post a YouTube video on Facebook in several different ways, using YouTube’s ‘Share’ feature*, Business Insider (Aug. 23, 2019), available at <https://www.businessinsider.com/how-to-post-a-youtube-video-on-facebook> (last accessed Apr. 15, 2021).



66. Additional factors make clear that social media applications are used in parallel to— rather than instead of—social networks. For one, many consumers use both YouTube and Facebook, rather than one over the other.³⁵ Social media applications make it easy for a user to share the content he or she finds on a social media application using his or her social network account. By clicking the “SHARE” button that appears underneath a video on YouTube, for example, YouTube pre-populates a hyperlink of the video that the user may then easily copy and paste on Facebook:³⁶



67. In addition, social networks, such as Facebook, provide specific product features to users which social media applications generally do not provide at all, much less in a “one-stop

³⁵ Federal Cartel Office Report, *supra*, ¶ 318 (noting that “Facebook.com and YouTube are increasingly used in parallel,” and that a “large number of [users utilize] YouTube without registration and thus solely for viewing videos.”).

³⁶ Gebel, *supra*.

shop.”³⁷ Social media applications, like YouTube and TikTok, do not provide or facilitate a similar use and instead offer only limited opportunities for social interaction, or interaction of a very different type that complements, rather than substitutes, for a social networking experience.

68. Since its initial market entry, in which it competed with early social networking companies such as Myspace and Friendster, Facebook has become dominant. Myspace has since ceased operating a social network—announcing that it “would no longer try to rival Facebook in social networking” and that it instead hoped to build a “social entertainment” site—while Friendster is defunct altogether.³⁸ Facebook, by contrast, has over 2.7 *billion* users worldwide, which is 42% of the global population (excluding China), including over 200 million users in the United States. As described in one recent article, “Facebook has been and remains the undisputed king of the social network market,” while other social networks—such as Diaspora—constitute “only a very small drop in the ocean compared to Facebook.”³⁹

69. There is both direct and indirect evidence of Facebook’s market power in the Social Network Market. An internal study conducted by Facebook itself concluded that “[f]or hundreds of millions of people today who want to connect with their friends and family, [Facebook is] the first—and more importantly—*only* choice.”⁴⁰

70. As the House Antitrust Subcommittee recently recognized, “the degree to which platforms have eroded consumer privacy without prompting a response from the market” is “evidence of platform market power[.]”⁴¹ Indeed, a social network’s “ability to maintain strong

³⁷ House Report, *supra*, at 91, 139 (noting that YouTube “is primarily used to consume video content online. It does not provide the core functionality of Facebook . . . such as Pages, Marketplace, or limited sharing within a person’s network.”).

³⁸ Whitney Kimball, *Why These Social Networks Failed So Badly*, Gizmodo (Aug. 19, 2019), available at <https://gizmodo.com/why-these-social-networks-failed-so-badly-1836996164> (last accessed Apr. 19, 2021).

³⁹ *What are the best alternatives to Facebook?*, IONOS Digital Guide (Jan. 14, 2021), available at <https://www.ionos.com/digitalguide/online-marketing/social-media/the-best-facebook-alternatives/> (last accessed Apr. 19, 2021).

⁴⁰ *State of New York et al v. Facebook, Inc.*, Case No. 1:20-cv-03589-JEB (D.D.C.), Dkt. 70, ¶ 242 (emphasis added).

⁴¹ House Report, *supra*, at 51.

1 networks while degrading user privacy can reasonably be considered equivalent to a monopolist's
 2 decision to increase prices or reduce product quality."⁴² Thus, "[a] firm's dominance can enable it
 3 to abuse consumers' privacy without losing customers."⁴³ Tellingly, during sworn testimony before
 4 the United States Congress regarding Facebook's data privacy lapses, Mark Zuckerberg—
 5 Facebook's founder and Chief Executive Officer—repeatedly struggled to name a single direct
 6 competitor to Facebook to whom consumers could turn.⁴⁴

7 71. As discussed more fully below, Facebook's market share in the Social Network
 8 Market is higher than its share in the Social Media Market and, in any event, exceeds 65%. In
 9 addition to this demonstrably high market share, Facebook has held this dominant share for years
 10 with high barriers to new entry (discussed further below). There is a reason a movie about
 11 Facebook is entitled, "*The Social Network*"; Facebook is far and away the dominant player in that
 12 market.

13 2) The Social Media Market

14 72. The Social Media Market is the product market consisting of social media
 15 applications and tools, which are websites and mobile applications that allow users of a given
 16 application to distribute various forms of media—such as text messages, photos, videos, and
 17 music—to other users of the same application.

18 73. Search engines, such as Google, Yahoo, or Bing, are not social media applications.⁴⁵
 19 That is because users primarily utilize search engines to find information that exists external from
 20 the search engine. A user might use Microsoft's Bing to search for "The New York Times" in
 21 order to find The New York Time's URL web address: "www.nytimes.com." By contrast, a user

22 ⁴² *Id.* at 52.

23 ⁴³ *Id.*

24 ⁴⁴ Sarah Jeong, *Zuckerberg struggles to name a single Facebook competitor*, The Verge
 25 (Apr. 10, 2018), available at <https://www.theverge.com/2018/4/10/17220934/facebook-monopoly-competitor-mark-zuckerberg-senate-hearing-lindsey-graham> (last accessed Apr. 19, 2021).

26 ⁴⁵ Relatedly, the United States Department of Justice ("DOJ") recently recognized that
 27 search engines are not "social media" in its recent antitrust complaint against Google. *See United*
 28 *States et al., v. Google LLC*, 1:20-cv-03010 (D.D.C.), Dkt. 1, ¶ 90 ("[P]latforms . . . are not
 reasonable substitutes for general search services.").

1 would utilize a social media application—such as YouTube—to find a video hosted on *that* social
2 media application.

3 74. Other forms of online entertainment are not reasonable substitutes for social media
4 applications because of the unique characteristics a social media application provides. TikTok, for
5 example, allows “users to express their ideas by sharing short videos with a broader community.”⁴⁶
6 By contrast, other services—including online cardrooms such as PokerStars—provide online
7 entertainment, but do so by means other than facilitating the distribution of various forms of media,
8 such as text messages, photos, videos, or music.

9 75. User behavior also confirms that social media applications are complements to other
10 types of online services and entertainment. Indeed, users utilize social media applications in
11 parallel to other online services and entertainment. A user may, for example, watch a Hulu-
12 produced show on Hulu, but use YouTube to share an amateur video review of that Hulu show.

13 76. In addition, social media applications offer an economic model that is distinct from
14 the economic models employed by other providers of other forms of online services and
15 entertainment, to the extent that the economic model may allow the option of not charging the user
16 a monetary fee. Indeed, many social media applications may not charge users a monetary price for
17 access to their applications, but subject the users to ads (for which advertisers monetarily
18 compensate the companies) or require the users to give up some form of limited data. By contrast,
19 other providers of online services and entertainment may collect from users a per-use monetary fee
20 or a regularly-occurring (monthly or annual) fee, but, as a result, may not serve them ads or may
21 not collect their data.

22 77. Direct evidence of Facebook’s monopoly power in the Social Media Market is
23 bountiful. For example, in an internal presentation prepared for Sheryl Sandberg, Facebook’s Chief
24 Operating Officer, Facebook maintained that “[t]he industry consolidates as it matures” and that
25 “Facebook is now 95% of all social media in the US[.]”⁴⁷ In another internal presentation,
26

27 ⁴⁶ House Report, *supra*, at 91.

28 ⁴⁷ House Report, *supra*, at 138.

Facebook noted that “[i]n every country we’ve tipped, we have maintained [market] penetration,” and it expressed skepticism that other firms could compete with Facebook.⁴⁸

78. In addition to direct evidence, there is also irrefutable indirect evidence of Facebook’s market power in the Social Media Market. Facebook is by far the largest social media company, and its market share exceeds 65%. In the United States, Facebook’s products include three of the seven most popular mobile apps, measured by monthly active persons, reach, and percentage of daily and monthly active persons.⁴⁹ Indeed, the House Antitrust Subcommittee’s recent report revealed that “[a]ccording to Facebook’s internal market data, its users spend significantly more time on its family of products than on competing services.”⁵⁰

79. Firms in the Social Media Market generate virtually all of their value to shareholders in the form of advertising revenue. Social media applications allow advertisers to use data about an application’s users in order to deliver targeted advertisements to consumers.

80. Facebook, Twitter, Snapchat, and other social media companies all compete for the attention and data of their users, which they then convert into revenue by selling advertising. Accordingly, one of the best available metrics of market share in the Social Media Market is advertising revenue. As reflected by its advertising revenue, Facebook (including Instagram) has over 85% of the U.S. market, with the second-place competitor, Twitter, claiming *less than 3.5%* market share.

81. Notably, one or more of Facebook services are considered a “must have” for most users, whereas other social media applications are not.⁵¹ This means that most social media users that are users of competing social media applications still have an account on a Facebook service (if not all of them), which further means that Facebook’s advertising revenues are a conservative estimate of its already obviously-dominant market share.

⁴⁸ *Id.* at 139.

⁴⁹ *Id.* at 136.

⁵⁰ *Id.* at 137–38.

⁵¹ Salvador Rodriguez, *TikTok passes Instagram as second-most popular social app for U.S. Teens*, CNBC (Oct. 6, 2020), available at <https://www.cnbc.com/2020/10/06/tiktok-passes-instagram-as-second-most-popular-social-app-for-us-teens.html> (last accessed Apr. 15, 2021).

1 **3) Relevant Geographic Market**

2 82. The United States is the relevant geographic scope of both the Social Media Market
3 and the Social Network Market. Social media applications each provide services to consumers
4 throughout the United States, and these services do not differ by geographic area within the United
5 States. For example, neither Facebook nor competing social media applications, such as YouTube,
6 limit the offering of their services to residents of San Jose, California, as opposed to residents of
7 Little Rock, Arkansas. On the other hand—due to multiple factors, including access to broadband
8 internet, switching costs, and consumer preferences—social media applications in other countries
9 are not reasonably interchangeable with applications in the Social Media Market. To the extent
10 that Facebook has competitors in the United States in the Social Network Market, the same is true
11 in that market as well.

12 **4) The Social Network and Social Media Markets Feature High Entry Barriers**

13 83. Facebook's monopoly is durable because it operates in an industry with strong
14 network effects and high barriers to entry.⁵² A network effect is the phenomenon by which the
15 value or utility a user derives from a good or service depends on the number of users of the same
16 good or service. Network effects may be either direct or indirect. Direct network effects arise
17 where a product or service becomes more valuable to users as additional others use the product or
18 service. Indirect network effects exist when greater use of a product or service incentivizes third
19 parties in a different customer group to also engage with that product or service.

20 84. As an example of direct network effects, take, for instance, a social media
21 application, such as YouTube. Even if the application has the very best features, the product is
22 worth comparatively little to a user if few other users utilize it to upload and view content.
23 Consumers use video applications like YouTube to find and disseminate content: the more users
24 who engage with it, the more valuable it becomes to each of them. The Social Media Market,
25 therefore, exhibits clear and obvious direct network effects. The direct network effects in the Social
26 Network Market are even stronger. Because users join a social network to interact with a large
27 number of their acquaintances, a social network cannot survive by providing access to content
28

⁵² See House Report at 37–45.

1 alone. Indeed, users will only utilize a given social network if it connects them with a large number
 2 of their social acquaintances, since “no person wants to be on a social network without other
 3 users.”⁵³

4 85. The powerful direct network effects inherent in the Social Network and Social
 5 Media Markets made competition at the early stages *for* the field rather than *within* the field.⁵⁴ The
 6 House Antitrust Subcommittee’s recent report recognized this point as it relates to Facebook,
 7 explaining that Facebook’s network effects are “very strong” and that “there are strong tipping
 8 points in the social networking market that create competition *for the market*, rather than
 9 competition within the market.”⁵⁵ A similar phenomenon has since made itself clear in the Social
 10 Media market, such that even though users may prefer to shift to non-Facebook options as their
 11 *favorite* (e.g., TikTok or Snap), they still engage most often with Facebook’s social media offerings
 12 (e.g., Instagram) because it is the dominant, “must have” social media application.⁵⁶

13 86. The content generated by Facebook’s user base also creates strong indirect network
 14 effects and, in turn, increases the value of the Facebook network to third parties, including
 15 developers and advertisers, and Facebook itself. Each photograph, relationship status, check-in, or
 16 post by a Facebook user rendered Facebook more valuable not only to users, but also to third parties,
 17 including advertisers and app developers, who seek to target content based on individuals’ data.
 18 This feedback loop enabled Facebook to use its anticompetitive strategy of consumer deception
 19 and monopolistic merger conduct to achieve a scale—bolstered by revenue from third parties such
 20 as advertisers and app developers that were drawn to Facebook—which substantially foreclosed
 21 competition in the Social Network and Social Media Markets.

22 87. Markets that exhibit strong network effects tend to be “sticky,” or accompanied by
 23 high switching costs. Once a significant number of users adopt a product, they will be reluctant to

24 ⁵³ *Id.* at 41.

25 ⁵⁴ *Id.*

26 ⁵⁵ *Id.* (emphasis added).

27 ⁵⁶ Salvador Rodriguez, *TikTok passes Instagram as second-most popular social app for U.S.*
 28 Teens, CNBC (Oct. 6, 2020), available at <https://www.cnbc.com/2020/10/06/tiktok-passes-instagram-as-second-most-popular-social-app-for-us-teens.html> (last accessed Apr. 15, 2021).

1 switch to even a superior competitive alternative, because the newer offering will not deliver as
 2 much value unless many other users make the switch simultaneously. This feature of network-
 3 effect markets produces a period of intense, early competition, after which a single, dominant player
 4 often becomes entrenched. Facebook itself suggested in an internal memorandum, with respect to
 5 social networks, “either everyone uses them, or no-one uses them.”⁵⁷ A fair and level playing field
 6 during the initial phase of early competition is thus crucial to maximize consumer welfare, as is a
 7 level playing field if a new type of social media application arises that threatens to supplant the old.

8 88. Switching costs impose a barrier to entry. To induce a user to adopt a new product
 9 in a market that has high switching costs, a competitor must incur not only the expense of building
 10 a superior product, but also the added compensation to defray a user’s cost of switching. An
 11 incumbent does not incur this added cost, retaining a cost advantage that is at least equal to the
 12 switching cost the competitor must absorb. Where switching costs are high, the incumbent’s
 13 competitive advantage is high as well.

14 89. High switching costs in the Social Network and Social Media Markets have allowed
 15 Facebook to prolong its monopoly. Facebook users may be connected to one another exclusively
 16 through Facebook’s network, leaving Facebook as the only method for users to remain in contact
 17 with one another. Faced with the possibility of losing contact with each other, Facebook users who
 18 would prefer to use another social media application or social network are largely prohibited from
 19 doing so because of these high switching costs.⁵⁸

20 90. Similarly, the lack of portability of Facebook users’ data presents an additional
 21 switching cost. To illustrate, “a user may upload a variety of data to Facebook, including photos
 22 and personal information, but (by Facebook’s design) may not be able to easily download the data
 23 and move it to another social media site; instead, the user would have to start from scratch, re-
 24 uploading her photos and re-entering her personal information to the new platform.”⁵⁹

25
 26 ⁵⁷ House Report, *supra*, at 141.

27 ⁵⁸ Srinivasan, *supra*, at 89.

28 ⁵⁹ House Report, *supra*, at 42.

91. Facebook’s tentacle-like grasp on other applications and services likewise presents yet another switching cost for consumers. For instance, users of the popular Spotify music streaming service frequently sign up for Spotify using their Facebook accounts.⁶⁰ But users who enroll in Spotify using their Facebook accounts “can’t disconnect it”—to use Spotify after leaving Facebook, users generally must set up new accounts on Spotify.⁶¹ In doing so, they lose access to their previous playlists, listening histories, connections with other users on Spotify, and other data.⁶² This discourages would-be defectors from leaving Facebook.

92. Monopolists who seek to deceive consumers and destroy competition can often be disciplined by market forces. A battery manufacturer, for example, that lies about the longevity of its batteries might be able to charge an unjustified premium price for a time. But as soon as the manufacturer’s deception is uncovered, consumers would quickly switch to a more fairly priced brand. However, the robust network effects present in the Social Network and Social Media Markets impeded market forces from overcoming Facebook’s market power once Facebook had anticompetitively secured its dominance. Consumers who discovered in 2018 that Facebook had not actually been protecting their privacy as it promised could not easily switch to an alternative, because their friends and connections were all on Facebook.

93. The Social Network and Social Media Markets feature other high barriers to entry, including significant initial investment. Once a social network and social media application like Facebook has achieved dominant market share, the amount of capital investment that would be required to challenge Facebook’s monopoly would be large. A potential competitor would not only have to build its own vast network with features Facebook does not offer, but would also have to pay users’ switching costs on a massive scale.

94. The accumulation of data presents another significant barrier to entry in the Social Network and Social Media Markets. Data has three defining properties which entrench the firms

⁶⁰ *Id.* at 146.

⁶¹ *Id.*

⁶² *Id.*

1 which accumulate it: volume, velocity, and variety.⁶³ Social networks and social media
 2 applications that amass a large volume of data from users are able to analyze data in a way that
 3 applications that do not collect vast (or any) data are not. Similarly, the velocity of data—the
 4 feedback loop between the collection and processing of data—allows social networks and social
 5 media applications to quickly identify and exploit the preferences, interests, activities, and contacts
 6 of their users. And, the variety of data that social networks and social media applications are able
 7 to collect—including (among other things) a user’s location, age, contact information, employment
 8 history, education level, computer-type, and relationship status—yields significant advantages that
 9 are difficult for potential competitors to overcome.

10 95. Coupled with the network effects and high barriers to entry in the Social Network
 11 and Social Media Markets, Facebook’s anticompetitive conduct allows it to extract supra-
 12 competitive rents from users in the form of personal data and attention and deliver minimum,
 13 suboptimal privacy protections and overall quality. Without these effects, users would switch to a
 14 competing social network that offered users greater data privacy, presented users with fewer ads,
 15 or provided users with richer content, features, or monetary compensation. Because of these
 16 barriers, however, Facebook has been able to reap supra-competitive profits from its
 17 anticompetitive conduct without the typical pressures of competition from existing competitors or
 18 new entrants. And, Facebook has been able to control and increase the amount of consumer
 19 information and attention that it demands.

20 96. Internal documents show that Facebook has been keenly aware of these market
 21 features. An internal memorandum prepared in October 2018 by a senior data scientist and
 22 economist at Facebook recognized that the network effects of Facebook and its products are “very
 23 strong.”⁶⁴ In another presentation, Facebook described its network effects as a “flywheel,”
 24 remarking that “[n]etwork effects make it very difficult to compete with us” and that its network

25 ⁶³ Ed Dumbill, *Volume, Velocity, Variety: What You Need to Know About Big Data*, Forbes
 26 (Jan. 1, 2019), available at <https://www.forbes.com/sites/oreillymedia/2012/01/19/volume-velocity-variety-what-you-need-to-know-about-big-data/?sh=50797c4d1b6d> (last accessed Apr.
 27 15, 2021).

28 ⁶⁴ House Report, *supra*, at 13, 13 n.14.

1 effects get “stronger every day.”⁶⁵ Similarly, Facebook’s founder, Mark Zuckerberg, has made
 2 clear Facebook’s recognitions that “[t]here are network effects around social products”; there are
 3 “a finite number of different social mechanics to invent” and “being first is how you build a brand
 4 and a network effect.”⁶⁶

5 97. Facebook’s own documents show its awareness that due to strong network effects
 6 and market tipping, Facebook is much less concerned with competition from other social apps in
 7 the market like Snapchat or Twitter, than from competition within Facebook’s *own* family of
 8 products—Facebook, Instagram, Messenger, and WhatsApp.⁶⁷ In the case of messaging apps,
 9 Facebook’s documents show that network effects can be even more extreme. And because
 10 Facebook is not interoperable with other social networks, its users face high costs to switch to other
 11 networks, locking them into Facebook’s network.

12 98. Facebook’s awareness of these features of the Social Network and Social Media
 13 Markets shaped its competitive strategy. For example, a senior executive at the company described
 14 its acquisition strategy as a “land grab,” while Zuckerberg has boasted that Facebook “can likely
 15 always just buy any competitive startups.”⁶⁸ Documents show that Facebook saw Instagram and
 16 WhatsApp as maverick competitors and their acquisitions as a way to protect and strengthen the
 17 durability of Facebook’s monopoly.⁶⁹

18 99. Upstart social media applications not only presented a competitive threat to
 19 Facebook in the Social Media Market, they also constituted potential entrants into the Social
 20 Network Market. Indeed, social media applications like Instagram and WhatsApp initially lacked
 21 the user base necessary to compete as a social network. They therefore focused on a relatively
 22 narrow niche in the Social Media Market in order to gain a foothold. As Instagram and WhatsApp
 23 added users and features, however, they began to build a combination of user base and functionality
 24

25 ⁶⁵ *Id.*

26 ⁶⁶ *Id.* at 143.

27 ⁶⁷ *Id.* at 384.

28 ⁶⁸ *Id.* at 12–13.

⁶⁹ *See id.* at 149, 160.

1 that could help them enter the Social Network Market and compete with Facebook in that market
2 as well.

3 100. Facebook's anticompetitive conduct, described more fully below, combined with
4 strong network effects and high barriers to entry, enabled it to obtain and maintain its monopolies
5 over the Social Network and Social Media Markets in the United States. As recognized by the
6 House Antitrust Subcommittee: "Facebook's monopoly power is firmly entrenched and unlikely to
7 be eroded by competitive pressures from new entrants or existing firms."⁷⁰

8 **D. Facebook Has Attempted to Acquire Market Power (and Has Succeeded in Acquiring**
9 **Market Power) by Deceiving Consumers about Its Privacy Practices.**

10 101. For years, Facebook has engaged in a pattern of deception about the amount of data
11 it obtains and the extent of the data harvesting and use by third parties its applications have long
12 enabled. Its deception has only recently begun to come to light.

13 102. Privacy practices were a crucial form of competition in the early days of the Social
14 Network and Social Media Markets. After its founding in 2003, Myspace quickly dominated the
15 Social Network and Social Media Markets. By 2006, Myspace supplanted Google as the most
16 visited website in the United States.

17 103. Myspace offered an "open" social network, allowing *all* interested users to join
18 Myspace. Moreover, Myspace users could sign up for Myspace using unverified usernames and
19 pseudonyms.

20 104. By 2007, overwhelmingly negative headlines began drawing attention to Myspace's
21 lax privacy practices. In particular, users, parents, and critics alike attributed sexual assaults,
22 suicides, and murders to Myspace, speculating that Myspace's open network—which cloaked
23 wrong-doers with relative anonymity, an added-level of covert protection—triggered these events.

24 105. By this time, competitors to Myspace—including Friendster, Orkut, Flip.com, Bebo,
25 and Facebook—had begun to emerge.

26 106. Given Myspace's prominence, Facebook sought to differentiate itself from Myspace
27 in order to entice users to join Facebook. Facebook initially distinguished itself on the basis of its
28

⁷⁰ *Id.* at 13.

1 strict privacy settings, including its closed-network approach. Importantly, Facebook promised
 2 users that it would disclose its “information and privacy practices” and that it would “not use
 3 cookies to collect private information from any user.”⁷¹

4 107. In 2006, some 250 million people around the world used a social network: 100
 5 million used Myspace, 12 million used Facebook, and the remainder used a number of other
 6 competitors.⁷² In 2007, user growth at Myspace began to come to a halt—by mid-2007, Facebook
 7 had begun to supplant Myspace as the most visited social network in the United States.⁷³

8 108. Facebook’s representations to consumers regarding its data policies were
 9 instrumental to Facebook gaining and maintaining market share at the expense of its rivals,
 10 including Myspace. A 2004 consumer survey revealed that a majority of Americans indicated that
 11 privacy was a “really important issue that [they] care about often.”⁷⁴ Another study focused on
 12 early Facebook users’ attitudes towards privacy, finding that they cared more about privacy policy
 13 than about terrorism.⁷⁵ Individuals in academia compared Facebook users’ satisfaction with
 14 Facebook’s privacy settings to Myspace users’ satisfaction with Myspace’s privacy settings,
 15 concluding that users typically preferred Facebook’s settings over Myspace’s.⁷⁶

16 109. Facebook itself recognized the importance that its supposed stringent privacy
 17 protections had in allowing Facebook to quickly amass dominance. In its 2008 internal report
 18 entitled “Facebook Secret Sauce,” Facebook recognized the nexus between its early success and its
 19 representations regarding privacy, explaining that “[u]sers will share more information if given
 20
 21
 22

23 ⁷¹ Srinivasan, *supra*, at 39. Cookies refer to small text files that websites can install on
 24 users’ computers, enabling them to remember and record users’ information. *Id.* at 49.

25 ⁷² *Id.* at 54.

26 ⁷³ *Id.*

27 ⁷⁴ *Id.* at 52 (brackets in original) (internal citation omitted).

28 ⁷⁵ *Id.* (internal citation omitted).

⁷⁶ *Id.*

1 more control over who they are sharing with and how they share.”⁷⁷ Similarly, in a November 2011
 2 post on Facebook, Zuckerberg recalled:

3 When I built the first version of Facebook, almost nobody I knew wanted a public
 4 page on the internet. That seemed scary. But as long as they could make their page
 5 private, they felt safe sharing with their friends online. Control was key. With
 6 Facebook, for the first time, people had the tools they needed to do this. *That’s how
 Facebook became the world’s biggest community online.*⁷⁸

7 110. To this day, consumers continue to care deeply about privacy. That is why many
 8 companies market their commitment to privacy as a selling point for their products and services.
 9 Apple, for instance, tells the public that “Apple believes that privacy is a fundamental human right”
 10 and that “[w]e share your belief that customers should have control over their data.”⁷⁹

11 111. Despite Facebook’s representations about its superior data privacy practices,
 12 Facebook spent the next fifteen years deceiving consumers about the data privacy protections that
 13 it provided to users in exchange for access to their data. When the scope of commercial
 14 surveillance—and the harvesting and use of user data—that Facebook’s practices enabled first
 15 began to be revealed in 2018 following news coverage about the Cambridge Analytica scandal,
 16 Facebook had already achieved monopolies in the Social Network and Social Media Markets.

17 112. Publicly, Facebook sought to differentiate itself by offering superior privacy
 18 protections. But behind the scenes—and entrenched in markets which provided additional
 19 protections to Facebook’s monopoly in the forms of powerful network effects, high switching costs,
 20 and other significant entry barriers—Facebook created a commercial surveillance infrastructure
 21 that enabled it to dominate its competitors. This would not have been possible if Facebook had not
 22 deceived consumers about its data privacy and commercial surveillance practices.

23
 24 ⁷⁷ *State of New York et al v. Facebook, Inc.*, Case No. 1:20-cv-03589-JEB (D.D.C.), Dkt.
 25 70, ¶ 76.

26 ⁷⁸ Anita Balakrishnan, Matt Hunter, & Sara Salinas, *Mark Zuckerberg has been talking*
 27 *about privacy for 15 years – here’s almost everything he’s said*, CNBC News (Apr. 9, 2018),
 available at <https://www.cnbc.com/2018/03/21/facebook-ceo-mark-zuckerbergs-statements-on-privacy-2003-2018.html> (last accessed Apr. 15, 2021) (emphasis added).

28 ⁷⁹ Apple Privacy Letter, *supra*.

113. In 2006, Facebook introduced News Feed. The curated feed was intended as a central destination so users did not have to browse through friends' profiles for updates. About one million users joined a "Facebook News Feed protest group," arguing the feature was too intrusive.⁸⁰

114. Facebook initially brushed off the criticism, but after continued outcry, Mark Zuckerberg issued a public apology, representing that "[w]hen I made Facebook two years ago . . . I wanted to create an environment where people could share whatever information they wanted, but also have control over whom they shared that information with" and urging that Facebook had "built extensive privacy settings – to give you even more control over who you share your information with."⁸¹ Importantly, Zuckerberg reassured Facebook users: "[t]his was a big mistake on our part, and I'm sorry for it. But apologizing isn't enough. I wanted to make sure we did something about it, and quickly. So we have been coding nonstop for two days to get you better privacy controls."⁸²

115. Facebook then instituted what it claimed were enhanced privacy settings that purportedly allowed users greater ability to keep their activities private.⁸³ For example, Facebook maintained that it would give users the option to block certain information—such as when a user removes profile information, posts on a Facebook Wall, comments on a photo, adds a friend, removes a relationship status, or leaves a group—from appearing on other users' News Feeds.⁸⁴ In announcing these updates, Facebook publicly assured users that "industry-leading privacy restrictions . . . have made Facebook a trusted site for sharing information."⁸⁵

⁸⁰ Alyssa Newcomb, *Can You Even Remember How You Coped Before Facebook's News Feed?*, NBC News, Sept. 26, 2016, available at <https://kl.link/2G1XF6Q> (last accessed Apr. 15, 2021).

⁸¹ Mark Zuckerberg, *An Open Letter from Mark Zuckerberg*, Facebook (Sept. 8, 2006), available at <https://www.facebook.com/notes/facebook/an-open-letter-from-mark-zuckerberg/2208562130/> (last accessed Apr. 18, 2021).

⁸² *Id.*

⁸³ See Facebook, *Facebook Launches Additional Privacy Controls for News Feed and Mini-Feed* (Sept. 8, 2006), available at <https://kl.link/3oq7BrY> (last accessed Apr. 15, 2021).

⁸⁴ *Id.*

⁸⁵ *Id.*

1 116. Despite claiming to provide users with enhanced privacy protections, however,
 2 Facebook increasingly made user data available to advertisers without disclosure to users.
 3 Facebook’s unrelenting deception of its users allowed Facebook to continue to amass market share
 4 in the Social Network and Social Media Markets.

5 117. Beginning in 2007, Facebook gave app developers access to user content and
 6 information, including content marked private.⁸⁶ As Facebook attempted “to become the world’s
 7 dominant social media service, it struck agreements allowing phone and other device makers access
 8 to vast amounts of its users’ personal information.”⁸⁷

9 118. Facebook did not disclose to its users the scope of the content and data that Facebook
 10 began providing to third parties at that early date, including user data marked “private.” But
 11 Facebook explained to third-party app developers in May 2007 that Facebook’s core value
 12 proposition and business model was “providing access to a new kind of data—social data, which
 13 enables you to build applications that are relevant to users.” With respect to that data, Facebook
 14 told developers: “You are on a level playing field with us. You can build robust apps, not just
 15 widgets. Complete integration into the Facebook site.”

16 119. Also in 2007, under the guise of “social advertisement,” Facebook introduced its
 17 “Beacon” product. Beacon allowed participating third parties to track users’ purchases outside
 18 Facebook and notify their Facebook friends.⁸⁸ As an illustration, when a Facebook user rented a
 19 movie from Blockbuster, the user would immediately receive a “pop-up” notification from
 20 Blockbuster requesting permission to share details regarding the user’s movie rental with
 21 Facebook.⁸⁹ Unless the user expressly declined permission by selecting the “No, Thanks” option,
 22 Facebook would receive information about the user’s rental activity (such as the movie title rented)

23 ⁸⁶ DCMS Report, *supra*, at ¶ 103.

24 ⁸⁷ Gabriel J.X. Dance, Nicholas Confessore, and Michael LaForgia, *Facebook Gave Device*
 25 *Makers Deep Access to Data on Users and Friends*, The New York Times (June 3, 2018), available
 at <https://kl.link/2HwXIYP> (last accessed Apr. 15, 2021).

26 ⁸⁸ Louise Story, *Facebook Is Marketing Your Brand Preferences (With Your Permission)*,
 27 The New York Times (Nov. 7, 2007), available at <https://kl.link/34tuzXy> (last accessed Apr. 15,
 2021).

28 ⁸⁹ Srinivasan, *supra*, at 56.

1 and publish that information on the user's Facebook page.⁹⁰ An example of a Beacon pop-up
 2 request displayed to Facebook users on third-party sites is pictured below:⁹¹



6 120. Many of Facebook's representations regarding its Beacon program were
 7 subsequently proven to be untrue. Facebook initially maintained that Beacon only tracked and
 8 maintained the activity of users that consented when prompted by the pop-up seeking permission.⁹²
 9 In reality, however, Beacon allowed Facebook to track the activity of even those users that clicked
 10 the "No, Thanks" prompt.⁹³

11 121. The FTC expressed concern about Facebook's Beacon program, and public outrage
 12 and litigation ensued.⁹⁴ Zuckerberg ultimately apologized, let users opt out, and called Beacon a
 13 mistake, reassuring Facebook users: "I'm not proud of the way we've handled this situation and I
 14 know we can do better."⁹⁵ Zuckerberg's statement represented that Facebook had learned its lesson
 15 and that it would not, in fact, use their data in unauthorized or intrusive ways.

16 122. As of the third quarter of 2008, Facebook had around 100 million monthly active
 17 users worldwide.⁹⁶ This placed it just behind Myspace, which had more than 110 million monthly
 18

21 ⁹⁰ *Id.*

22 ⁹¹ *Id.*

23 ⁹² *Id.* at 57.

24 ⁹³ *Id.* at 58.

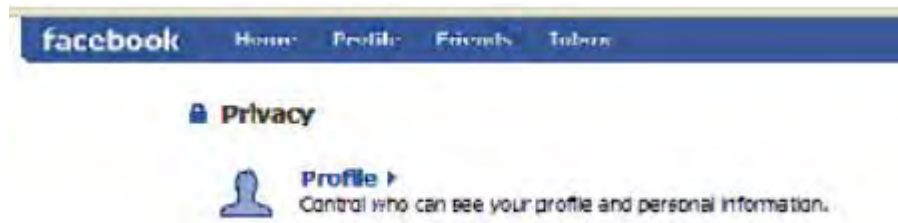
25 ⁹⁴ *See id.* at 57–59.

26 ⁹⁵ Betsy Schiffman, *Facebook CEO Apologizes, Lets Users Turn Off Beacon*, Wired (Dec. 5, 2007), available at <https://www.wired.com/2007/12/facebook-ceo-apologizes-lets-users-turn-off-beacon/> (last accessed Apr. 20, 2021).

27 ⁹⁶ *Number of monthly active Facebook users worldwide as of 4th quarter 2020*, Statista, available at <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> (last accessed Apr. 15, 2021).

1 active users.⁹⁷ Facebook passed Myspace in terms of monthly active users in the United States in
 2 2009. Myspace never came close to Facebook again, although it continued to exist as a competitor
 3 through 2014.

4 123. In or around November 2009, Facebook began providing its users with a “Central
 5 Privacy Page,” which contained a “Profile” link and accompanying text representing that a user
 6 could “[c]ontrol who can see your profile and personal information.”⁹⁸ An example of Facebook’s
 7 “Central Privacy Page” is pictured below:



12 124. By 2010, bolstered by its ostensible commitment to privacy, Facebook had become
 13 the largest social network in the world. However, unknown to nearly all of its users, Facebook had
 14 transitioned its business to selling access to data, which it did by selling access to developers and
 15 selling advertisements targeting Facebook’s network of engaged and active users. In March 2010,
 16 it was reported that Facebook had booked revenues of up to \$700 million in 2009 and was on track
 17 for \$1.1 billion in 2010—almost all from advertising to its users. Facebook had been roughly
 18 doubling its revenues every year up until that point—\$150 million in 2007; nearly \$300 million in
 19 2008; and \$700 million in 2009.

21 125. In early 2010, Facebook launched its “Like” button, which is also referred to as a
 22 “Social Plugin.” The “Like” button is a web plug-in that appears on a third party’s website. If a
 23 user supports or “likes” a particular piece of content on a third party’s website—such as a particular
 24 news article—a number ticker besides the “Like” button increases by one. A preview of the content
 25

26 ⁹⁷ Jeremiah Owyang, *Social Network Stats: Facebook, MySpace, Reunion (Jan, 2008)*,
 27 <https://web-strategist.com/blog/2008/01/09/social-network-stats-facebook-myspace-reunion-jan-2008/> (last accessed Apr. 15, 2021).

28 ⁹⁸ DCMS Report, *supra*, ¶ 65.

1 that the Facebook user “liked” on a third party’s website may appear to the user’s followers on
 2 Facebook in the user’s News Feed, potentially drawing additional viewers to visit the third-party
 3 website after observing the previewed content in the user’s News Feed. A version of Facebook’s
 4 “Like” button that appears on third-party websites is pictured below:⁹⁹



7 126. Marketed as a way to share opinions, the Like button in reality enabled Facebook to
 8 obtain consumer data by tracking activity across the internet. At the time that Facebook launched
 9 its “Like” button, Facebook’s “Frequently Asked Questions” page indicated that “No data is shared
 10 about you when you see a social plug-in on an external website.”¹⁰⁰ Independent researchers
 11 subsequently determined, however, that the presence of the “Like” button on third-party websites
 12 allowed Facebook to monitor users and obtain their data anytime users visited those third-party
 13 websites, even when users did *not* click the “Like” button.¹⁰¹

14 127. Investigators soon uncovered this deception, and Facebook settled with the FTC to
 15 resolve the agency’s charges that “Facebook deceived consumers by telling them they could keep
 16 their information on Facebook private, and then repeatedly allowing it to be shared and made
 17 public.”¹⁰² Facebook’s settlement with the FTC barred Facebook from making any further
 18 deceptive privacy claims, required Facebook to get consumers’ approval before it changes the way
 19 it shared their data, and required Facebook to obtain periodic assessments of its privacy practices
 20 by independent, third-party auditors for the next 20 years.

21 128. In particular, under the settlement, Facebook was specifically:

22 _____
 23 ⁹⁹ Ray C. He, *Introducing new Like and Share buttons*, Facebook for Developers News
 24 (Nov. 6, 2013), available at <https://developers.facebook.com/blog/post/2013/11/06/introducing-new-like-and-share-buttons/> (last accessed Apr. 15, 2021).

25 ¹⁰⁰ Declan McCullagh, *Facebook ‘Like’ button draws privacy scrutiny*, CNET (June 2,
 26 2010), available at <https://www.cnet.com/news/facebook-like-button-draws-privacy-scrutiny/> (last
 27 accessed Apr. 15, 2021).

28 ¹⁰¹ Srinivasan, *supra*, at 65–67.

¹⁰² Press Release, Federal Trade Commission, Facebook Settles FTC Charges That It
 Deceived Consumers By Failing To Keep Privacy Promises (Nov. 29, 2011), available at
<https://kl.link/3mqWAEX> (last accessed Apr. 15, 2021).

1 a) barred from making misrepresentations about the privacy or security of
2 consumers' personal information;

3 b) required to obtain consumers' affirmative express consent before enacting
4 changes that override their privacy preferences;

5 c) required to prevent anyone from accessing a user's material more than 30
6 days after the user has deleted his or her account;

7 d) required to establish and maintain a comprehensive privacy program
8 designed to address privacy risks associated with the development and management of new and
9 existing products and services, and to protect the privacy and confidentiality of consumers'
10 information; and

11 e) required, within 180 days, and every two years after that for the next 20
12 years, to obtain independent, third-party audits certifying that it has a privacy program in place that
13 meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers'
14 information is protected.¹⁰³

15 129. Ultimately, however, Facebook did not comply with its promises to the FTC.

16 130. In response to these controversies, and as another example of the promises that
17 Facebook made—but subsequently did not keep—regarding its privacy protections, Facebook
18 announced in 2012 that future privacy changes would require user approval through voting.¹⁰⁴
19 During a “privacy press conference,” Facebook founder Mark Zuckerberg explained that Facebook
20 is “one of the only services on the web where people are sharing pretty personal and intimate
21 information”; that requiring users' approval for privacy changes “mak[es] it so that we can't just
22 put in a new terms of service without everyone's permission”; and that “[w]e think these changes
23 will increase the bonding and trust users place in the service.”¹⁰⁵ But, consistent with its pattern of
24

25 ¹⁰³ *Id.*

26 ¹⁰⁴ Eyder Peralta, *Facebook Will Allow Users to Vote On Privacy Changes*, NPR (June 1,
27 2012), available at <https://www.npr.org/sections/thetwo-way/2012/06/01/154162976/facebook-will-allow-users-to-vote-on-privacy-changes> (last accessed Apr. 15, 2021).

28 ¹⁰⁵ Srinivasan, *supra*, at 61–62.

1 deception, Facebook ultimately did not keep that commitment, choosing to end the process of
2 requiring users' approval for future privacy changes.¹⁰⁶

3 131. Facebook's continued promises regarding privacy negatively impacted potential
4 rivals—even those backed by the largest companies in the world—from ever gaining appreciable
5 market share. In 2010, Google launched a new social network, Google+. Google+ was Google's
6 attempt to build out a “social graph” that would leverage a common user identity across Google
7 products, including YouTube and Gmail.

8 132. With Google+, Google sought to surpass the essential product features and
9 functionality of Facebook. The planned features for Google+ included a continuous scroll product
10 called the “stream”; a companion feature called “sparks,” which related the “stream” to users'
11 individual interests; and a sharing app called “Circles” to share information with one's friends,
12 family, contacts, and the public at large.

13 133. Google+ represented a massive investment of resources to bring a finished, full-
14 scale social network to market. Google conscripted almost all of the company's products to help
15 build Google+. At its peak, Google+ involved 1,000 employees from divisions across the country.
16 Google even required employees to use the Google+ Hangouts video chat feature, which was
17 supposed to help drive adoption in the tech industry and beyond.

18 134. Facebook knew that many users would switch to Google+ if they thought Facebook
19 offered inferior privacy protections. The competitive threat of Google+ (while it lasted) therefore
20 temporarily prevented Facebook from even further eroding its privacy features. In 2011, for
21 example, Facebook allowed its users to “untag” themselves from photographs, even where another
22 user had “tagged” them in the first place.¹⁰⁷ Facebook had planned to eliminate this feature which
23 allowed users to “untag” themselves, but feared that this change would welcome controversy since
24 Facebook's planned change would reduce its users' privacy. Indeed, one Facebook executive

25 ¹⁰⁶ Dave Lee, *Facebook criticised over decision to stop public privacy votes*, BBC News
26 (Nov. 22, 2012), available at <https://www.bbc.com/news/technology-20444678> (last accessed Apr.
27 15, 2021).

28 ¹⁰⁷ *State of New York et al v. Facebook, Inc.*, Case No. 1:20-cv-03589-JEB (D.D.C.), Dkt.
70, ¶ 95.

1 explained: “IF ever there was a time to AVOID controversy, it would be when the world is
 2 comparing our offerings to G+.”¹⁰⁸ The same executive subsequently advised that Facebook
 3 postpone any changes to its privacy policies “until the direct competitive comparisons begin to die
 4 down.”¹⁰⁹

5 135. Google’s attempt to compete with Facebook, ultimately failed, however. Even
 6 though Google+ continued as a competitor until 2018, it was never able to dethrone Facebook or
 7 take appreciable market share away from Facebook, all the while Facebook continued to mislead
 8 users in order to prevent them from switching to a network that offered similar features, but with
 9 better actual privacy practices.

10 136. Facebook’s deception about its data privacy practices and anticompetitive string of
 11 acquisitions drove the rapid growth of Facebook’s ever-increasing user base and increased the value
 12 of Facebook’s social graph. As Facebook’s VP of Product Management explained to Mark
 13 Zuckerberg in an October 2012 email, the data that Facebook collects has made Facebook
 14 progressively better at collecting and monetizing consumer data: “We know more about what
 15 people want to see because people look at more stuff on our platform . . . the more people that use
 16 the system, the more information we have on how to make more people use the system.”

17 137. Facebook went public in 2012. In pursuit of revenue, Facebook began using “View
 18 Tags,” which allow advertisers to track Facebook users across the Internet using cookies.¹¹⁰
 19 Facebook also gave advertisers the ability to conduct more fine-grained bidding for advertising and
 20 to advertise specifically to a “custom audience”—*i.e.*, a list of specific users provided by the
 21 advertiser. Facebook did not disclose that its user data practices allowed third parties to track
 22 Facebook users across the internet using cookies.

23
24
25
26 ¹⁰⁸ *Id.*

27 ¹⁰⁹ *Id.*

28 ¹¹⁰ Rebecca Greenfield, *2012: The Year Facebook Finally Tried to Make Some Money*, The Atlantic (Dec. 14, 2012), available at <https://kl.link/34qhxdd> (last accessed Apr. 15, 2021).

1 138. At the time of Facebook’s 2012 initial public offering (“IPO”), its filings with the
 2 Securities and Exchange Commission (“SEC”) indicated that the company had 845 million monthly
 3 active users and that its website featured 2.7 billion daily likes and comments.¹¹¹

4 139. Facebook later combined user content with other third-party data, thereby de-
 5 anonymizing the third-party data. For example, in April 2013, Facebook created information
 6 dossiers on millions of users and non-users alike. The dossiers even included names, health
 7 information, information about neighbors, and proclivities. Facebook did not disclose the dossiers
 8 to users (or even the fact of the dossiers’ existence), using them instead to allow advertisers to target
 9 users with more precision.¹¹² Users were unaware of the extent of Facebook’s commercial
 10 surveillance and did not first begin to become aware until the news of the Cambridge Analytica
 11 scandal broke—in March 2018, the overwhelming majority of Facebook users incorrectly believed
 12 Facebook collected data only when logged in.¹¹³

13 140. Facebook engaged in this continued pattern of deception with the specific intent to
 14 monopolize the Social Network and Social Media Markets and ultimately to maintain and exploit
 15 its monopoly. Facebook succeeded in deceiving consumers long enough to solidify its market
 16 power in the Social Network and Social Media Markets. By the time Facebook’s deception about
 17 its subpar data privacy practices was revealed in 2018—*i.e.*, the year Google+ left the market due
 18 to inability to grow—it had achieved unrivaled dominance.

19 **E. The Cambridge Analytica Scandal Partially Reveals the Extent of Facebook’s**
 20 **Deception.**

21 141. It was not until the Cambridge Analytica scandal in 2018, that consumers first began
 22 to discover the scope and implications of Facebook’s lax data privacy practices. In particular, the
 23 scandal revealed that Facebook had been giving app developers the ability to harvest Facebook

24 _____
 25 ¹¹¹ Facebook’s Form S-1 Registration Statement under the Securities Act of 1933,
<https://kl.link/2L9TgRD> (last accessed Apr. 15, 2021).

26 ¹¹² Tim Peterson, *Facebook Will Remove Advertisers’ Other Third-Party Data Option, But*
 27 *Loopholes, Questions Remain*, DigiDay (Apr. 6, 2018), available at <https://kl.link/37Mprij> (last
 28 accessed Apr. 15, 2021).

¹¹³ Paul Hitlin & Lee Rainie, *Facebook Algorithms and Personal Data*, Pew Research
 Center (Jan. 16, 2019), available at <https://kl.link/37EsidN> (last accessed Apr. 15, 2021).

1 users' private data without the users' consent, and to use that data for purposes beyond targeted
2 advertising on Facebook.

3 142. Cambridge Analytica ("CA") was a British political consulting firm that combined
4 data harvesting and analytics for use in political advertising. A CA app known as "This Is Your
5 Digital Life" presented users with a series of questions that were used to build a psychological
6 profile on users. The app harvested data not only from the app users' own apps, but also from the
7 users' Facebook friends.

8 143. CA's practices were uncovered in March 2018, when it was revealed that, based on
9 the 270,000 Facebook users who used the CA app, CA was able to access the personal data of up
10 to 87 *million* Facebook users. The vast majority of these users had not given CA permission to
11 access their data.

12 144. After the scandal broke, Facebook banned the app and claimed that CA had breached
13 Facebook's terms of service.¹¹⁴ However, an investigation revealed that, as early as April 2015,
14 Facebook recognized that it was unable to keep track of how many app developers were using
15 previously downloaded data.¹¹⁵ And Facebook's data permissions allowed apps to access data not
16 only about an app user, but about all of the app user's friends.

17 145. As early as at least 2010, Facebook deceptively allowed third parties to access the
18 data of a Facebook user's friends, and this policy formed part of the basis for the FTC's 2011
19 complaint. In 2012, however, as part of its settlement with Facebook, the FTC ordered that
20 Facebook "shall not misrepresent in any matter, expressly or by implication, the extent to which
21 [Facebook] maintains the privacy or security of Covered Information, including . . . [Facebook's
22 collection, use, or disclosure of any Covered Information[.]" In 2015, Facebook further represented
23 to users that it was ending the practice of allowing third parties to access the data of users' friends.

24
25 ¹¹⁴ Kurt Wagner, *Here's how Facebook allowed Cambridge Analytica to get data for 50*
26 *million users*, Vox (Mar. 17, 2018), available at <https://kl.link/2ToOFLZ> (last accessed Apr. 15, 2021).

27 ¹¹⁵ Deepa Seetharaman and Kirsten Grind, *Facebook's Lax Data Policies Led to Cambridge*
28 *Analytica Crisis*, The Wall Street Journal (Mar. 20, 2018), available at <https://kl.link/3jt8o86> (last accessed Apr. 15, 2021).

Contrary to Facebook’s representation, however, and in breach of its 2012 settlement with the FTC, most third parties could continue to access this data. The volume of data these third parties acquired from Facebook led one Facebook employee to remark: “I must admit, I was surprised to find out that we are giving out a lot here for no obvious reason.”¹¹⁶

146. Until at least 2018, Facebook still allowed some number of third parties to access the data of users’ friends. The DOJ expressly noted Facebook’s falsehoods regarding its sharing its users’ data in its 2019 complaint against Facebook for Facebook’s breach of its 2012 settlement agreement with the FTC.¹¹⁷ It was only after news of the Cambridge Analytica scandal broke that Facebook’s continued deception regarding its sharing of the data of its users’ friends began to come to light. In its 2019 complaint against Facebook, the DOJ cautioned that “[t]he full scale of unauthorized collection, use, and disclosure of consumer information resulting from Facebook’s conduct is unknown due, at least in part, to the company’s lack of recordkeeping.”¹¹⁸

147. By this time in 2018, however, Facebook’s social network and social media monopolies were fully entrenched with over 217 million users in the United States. That year, Facebook earned over \$55 billion in revenue, almost completely from selling targeted advertising made more valuable to Facebook and third parties due to a lack of meaningful data privacy protections.

148. In September of 2019, Facebook said it suspended tens of thousands of apps for improperly taking users’ personal data and other transgressions, “a tacit admission that the scale of its data privacy issues was far larger than it had previously acknowledged.”¹¹⁹ Facebook eventually disclosed that it had suspended 69,000 apps, and 10,000 of those apps were flagged for potentially

¹¹⁶ *United States v. Facebook, Inc.*, Case No. 1:19-cv-02184 (D.D.C.), Dkt. 1, ¶ 84.

¹¹⁷ *Id.*, ¶¶ 5–9.

¹¹⁸ *Id.*, ¶ 126.

¹¹⁹ Kate Kogner, Gabriel J.X. Dance, and Mike Isaac, *Facebook’s Suspension of ‘Tens of Thousands’ of Apps Reveals Wider Privacy Issues*, *The New York Times* (Sept. 20, 2019), available at <https://kl.link/31JmImH> (last accessed Apr. 15, 2021).

misappropriating personal data from Facebook users.¹²⁰ The scale and scope of Facebook’s data privacy issues made clear that its lackluster data privacy protections were a feature, not a bug, of Facebook’s social network.

149. On July 24, 2019, the FTC and the DOJ announced that Facebook would pay a \$5 billion penalty, and submit to new restrictions and a modified corporate structure, to settle charges that the company had “deceiv[ed] users about their ability to control the privacy of their personal information.”¹²¹

150. The largest penalty ever imposed by the FTC before that time was \$275 million. The FTC explained: “Facebook monetizes user information through targeted advertising, which generated most of the company’s \$55.8 billion in revenues in 2018. To encourage users to share information on its platform, Facebook promises users they can control the privacy of their information through Facebook’s privacy settings.”¹²²

151. The FTC further explained that despite Facebook’s representations, “Facebook repeatedly used deceptive disclosures and settings to undermine users’ privacy preferences,” determining that “[t]hese tactics allowed the company to share users’ personal information with third-party apps that were downloaded by the user’s Facebook ““friends,”” and further finding that “Facebook took inadequate steps to deal with apps that it knew were violating its platform policies.”¹²³

152. The FTC’s 2019 charges made clear that Facebook had egregiously violated the FTC’s 2012 order by repeatedly using deceptive disclosures and settings to undermine users’ privacy preferences. In testimony to the United Kingdom’s House of Commons, the FTC’s former Chief Technologist—Ashkan Soltani—recognized that “time and time again Facebook allows

¹²⁰ See Facebook, *An Update on Our App Developer Investigation* (Sept. 20, 2019), available at <https://kl.link/31FSVeP> (last accessed Apr. 15, 2021).

¹²¹ Federal Trade Commission, *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, available at <https://kl.link/34snVR0> (last accessed Apr. 15, 2021).

¹²² *Id.*

¹²³ *Id.*

1 developers to access personal information of users and their friends, in contrast to their privacy
2 settings and their policy statements.”¹²⁴

3 153. In the aftermath of its 2012 settlement with the FTC, Facebook promised that it
4 would give consumers “clear and prominent” notice and obtain their consent before sharing their
5 information beyond those entities clearly enumerated in consumers’ privacy settings.¹²⁵ If a
6 Facebook user, for example, curated his or her privacy settings to designate that particular
7 content—such as photos—be visible only to the user’s “friends,” Facebook represented—and the
8 2012 FTC settlement required—that Facebook would obtain the user’s “affirmative express
9 consent” before sharing that content beyond the user’s “friends.”¹²⁶

10 154. Consumers relied on Facebook’s representations before and after the aftermath of
11 its 2012 settlement with the FTC in deciding to continue to use Facebook (rather than its
12 competitors) and to give Facebook access to their personal data in exchange for use of Facebook.
13 But by the time consumers learned that Facebook had violated that settlement, they could not
14 reasonably switch to a comparable social network or social media application. Facebook had
15 already achieved monopoly power in the Social Network and Social Media Markets, and network
16 effects, high barriers to entry, and immense switching costs made it more likely that Facebook’s
17 monopolies would be maintained. Although market forces can sometimes reign in companies that
18 deceive users, the Social Network and Social Media Markets’ unique features made it more difficult
19 for the market to discipline Facebook for violating its commitments to consumers.

20 155. Notwithstanding widespread outrage after the Cambridge Analytica scandal, the
21 vast majority of Facebook users have continued to use Facebook and its family of products. The
22 reason for this is clear. As Facebook was keenly aware, a social network really only has value if
23

24 ¹²⁴ DCMS Report, *supra*, ¶ 89.

25 ¹²⁵ Frederic Lardinois, *Facebook And FTC Settle Privacy Charges—No Fine, But 20 Years*
26 *Of Privacy Audits*, TechCrunch (Aug. 10, 2012), available at <https://techcrunch.com/2012/08/10/facebook-ftc-settlement-12/> (last accessed Apr. 1, 2021).

27 ¹²⁶ Somini Sengupta, *F.T.C. Settles Privacy Issue at Facebook*, The New York Times (Nov.
28 29, 2011), available at <https://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html> (last accessed Apr. 1, 2021).

1 users' friends use it too. And once a social network reaches critical mass, it entrenches itself in the
 2 the market, and users generally no longer have a viable alternative to the social graph, "as there is
 3 no reason for users to start using a social network if there is no one there with whom they can
 4 connect."¹²⁷ Thus, notwithstanding widespread outrage after the Cambridge Analytica scandal,
 5 few Facebook users stopped using Facebook, because there was no longer any other viable network
 6 to use.

7 **F. Facebook Uses Anticompetitive Acquisitions and Threats to Destroy Competition in**
 8 **the Social Network and Social Media Markets.**

9 156. Facebook also sought to protect and expand its monopolies by regularly destroying
 10 and acquiring competitive threats, and it used its market power and data advantage to
 11 anticompetitively achieve its monopolistic objectives.

12 157. Since its founding in 2004, Facebook has acquired at least 63 companies.¹²⁸ While
 13 those acquisitions have been public, the public has only recently discovered the extent to which
 14 Facebook used the data it deceptively obtained from users to identify nascent competitors and target
 15 them for acquisition or destruction. This new information has shown that Facebook's
 16 anticompetitive acquisitions were enabled by, and the result of, Facebook's deceptive privacy
 17 practices.

18 **1) Facebook's Tracking of Consumers Drove Its Copy, Acquire, or Kill Strategy.**

19 158. Facebook used data that it obtained from users to track the websites and apps visited
 20 by its users—often without full disclosure—to identify which upstart competitors were gaining
 21 traction so that it could target them for acquisition or destruction. Facebook "led a sustained effort
 22 to surveil smaller competitors to benefit Facebook . . . steps taken to abuse data, to harm
 23 competitors, and to shield Facebook from competition."¹²⁹ In fact, Facebook intentionally
 24 developed its ability to surveil users to aid its acquisition strategy, which has continued from the
 25 point at which it first emerged as the largest social network through today.

26 ¹²⁷ House Report, *supra*, at 89.

27 ¹²⁸ *Id.* at 149.

28 ¹²⁹ *Id.* at 166.

1 159. Historically, Facebook used its own internal data and data from Comscore, a data
2 analytics and measurement firm, to track the growth of competitive threats.¹³⁰ But Facebook’s
3 efforts were only as good as that underlying data. Facebook therefore decided to capture more
4 robust data from its users through increased surveillance so that it could remove future competitors
5 from the social network and social media chessboards.

6 160. In April 2012, Facebook’s Director of Growth, Javier Olivan, emailed Zuckerberg
7 and Chris Cox, Facebook’s Chief Product Officer, about improving Facebook’s “competitive
8 research.” Olivan indicated that “getting our data in great shape is going to require effort,” but that
9 Facebook’s building its own system for identifying competitive threats would “allow us to get 10x
10 better at understanding” competitive threats to Facebook’s dominance of mobile devices.¹³¹ Olivan
11 explained:

12 I keep seeing the same suspects (instagram, pinterest, ...) [sic] both on our
13 competitive radar / platform strategy as wins . . . I think having the exact data about
14 their users [sic] engagement, value they derive from [Facebook] . . . would help us
15 make more bold decisions on whether they are friends or foes. Back to your thread
16 about “copying” vs. “innovating” we could also use this info to inspire our next
17 moves.¹³²

18 161. Zuckerberg responded “Yeah, let’s do it.” Underscoring the importance to
19 Facebook of utilizing its users’ data to identify competitive threats, Zuckerberg committed to
20 “find[ing] some time periodically during my weekly reviews to go over this stuff.”¹³³

21 162. In 2013, Olivan approached Zuckerberg about the prospect of Facebook acquiring
22 Onavo, an Israeli mobile web analytics company that ran a virtual private network (“VPN”). A
23 VPN provides security and encryption to a user, creating a “data tunnel” which cloaks data when
24

25 ¹³⁰ *Id.* at 160–66.

26 ¹³¹ *Id.* at 161.

27 ¹³² *Id.*

28 ¹³³ *Id.*

1 sent over the user’s internet connection, scrambling the user’s online activity from detection by
 2 third parties.¹³⁴

3 163. At that time, Olivan urged Zuckerberg that Onavo could provide Facebook powerful
 4 “competitive insights” that were “really cool for identifying acquisition targets.”¹³⁵ According to
 5 Olivan, “Onavo makes sense strategically since it solves the mobile market data problem 10x better
 6 than any other alternative – and you know how important this data becomes any time we have
 7 engagement or competition questions[.]”¹³⁶

8 164. Facebook acquired Onavo in October 2013 for \$115 million. Prior to acquiring
 9 Onavo, Facebook had relied on Onavo’s surveillance of Facebook’s competitors for years, such as
 10 during the process of acquiring Instagram, and Facebook ultimately acquired and used Onavo’s
 11 assets to track potential competitors through non-public, internal, real-time data about its users’
 12 engagement, usage, and time spent on other apps.¹³⁷ Tellingly, at the time it acquired Onavo,
 13 Facebook did *not* intend to place Onavo’s employees in Facebook’s Data Analytics team. Instead,
 14 in acquiring Onavo, Facebook planned to place Onavo’s employees, including its cofounder, Guy
 15 Rosen, under Facebook’s Growth team, reporting to Javier Olivan.¹³⁸

16 165. Onavo allowed Facebook to surreptitiously gather information from consumers who
 17 used Onavo’s mobile applications by representing that these applications provided data security
 18 features. The types of information that Facebook collected through Onavo include (among others)
 19 “every app the user has accessed”; “the number of seconds the user spent in the app per day”; “the
 20 percent of time the user spent in a specific app out of their total mobile usage time”; “the actions
 21 taken by the user in each app”; and personal information such as the user’s country of origin, age,

22 ¹³⁴ Steve Symanovich, *What is a VPN?*, NortonLifeLock (Jan. 14, 2021), available at
 23 <https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html> (last accessed Apr. 19, 2021).

24 ¹³⁵ See *State of New York et al v. Facebook, Inc.*, Case No 1:20-cv-03589-JEB (D.D.C.),
 Dkt. 70, ¶ 141.

25 ¹³⁶ *Id.*

26 ¹³⁷ Betsy Morris and Deepa Seetharaman, *The New Copycats: How Facebook Squashes*
 27 *Competition From Startups*, The Wall Street Journal (Aug. 9, 2017), available at
<https://kl.link/3e6nMpW> (last accessed Apr. 15, 2021).

28 ¹³⁸ House Report, *supra*, at 161.

1 and gender.¹³⁹ Facebook weaponized the near-instantaneous information it obtained through
2 Onavo to identify competitors to “copy, acquire, or kill.”

3 166. Facebook immediately began integrating Onavo’s applications into both its business
4 operations and its acquisition strategy. Facebook, for example, began analyzing data secretly
5 collected from Onavo’s Protect software, which was a massive surveillance and data collection
6 scheme disguised as VPN software. Cynically marketed to consumers as a way to, *inter alia*,
7 “keep you and your data safe,” “Save, Measure & Protect your mobile data,” “help[] you take
8 charge of how you use mobile data and protect your personal info,” “[a]dd an extra layer of
9 protection to all your mobile data traffic for additional security,” and provide “Peace of Mind When
10 You Browse,” Onavo Protect in fact monitored all web and mobile application traffic on a user’s
11 mobile device and ultimately redirected that information to Facebook, where it was logged and
12 analyzed by Facebook’s product teams.¹⁴⁰ By February 2018, Onavo apps had been downloaded
13 thirty-three million times across both iOS and Android.

14 167. Facebook has used extensive surveillance of users to identify and target nascent
15 competitive threats. Using the data it obtained from Onavo and other sources, Facebook then
16 eliminated upstart competitors by demanding concessions in agreements, by denying access to vital
17 sources of data and information on Facebook’s network, or by acquisition. As elected officials
18 have recognized, the technology Facebook obtained from Onavo and other data brokers allowed
19 Facebook to protect and further its market dominance:¹⁴¹



20 Congresswoman Pramila Jayapal

21 July 29, 2020 ·

22 Facebook is a case study in monopoly power: It harvests and monetizes our data, then uses it to spy on competitors—to copy,
23 acquire, and kill rivals.

24 This destructive model makes it impossible for new companies to flourish—harming our democracy, small businesses, and
25 consumers.

26 ¹³⁹ *Australian Competition & Consumer Commission v. Facebook, Inc. et al*, Federal Court
27 of Australia (Dec. 16, 2020), ¶ 11, available at [https://www.accc.gov.au/
28 system/files/ACCC%20v%20Facebook%20Inc%20%26%20Ors_%20Concise%20Statement_0.p
df](https://www.accc.gov.au/system/files/ACCC%20v%20Facebook%20Inc%20%26%20Ors_%20Concise%20Statement_0.pdf) (last accessed Mar. 29, 2021) (“ACCC Complaint”).

¹⁴⁰ *Id.*, at Annexure A1–A4.

¹⁴¹ United States Representative Pramila Jayapal, Facebook (July 29, 2020), available at
<https://www.facebook.com/RepJayapal/videos/questioning-mark-zuckerberg/319712279065223/>
(last accessed Apr. 19, 2021).

168. Some of the ways that Facebook exploited users' data that Facebook obtained from Onavo or other sources to inform Facebook's anticompetitive "copy, acquire, kill" strategy are detailed below. Like a football team that stole other teams' play calls, Facebook used its deceptive surveillance of users to know precisely which competitors to pick off. Notably, however, the extent to which Facebook used ill-gotten user data to pursue these strategies was not known until recently.

2) Facebook Threatened Competitors with Discriminatory Practices to Help Drive its Anticompetitive Acquisition Strategy.

169. In addition to the surveillance Facebook conducted through Onavo, Facebook's "copy, acquire, kill" strategy was also built on the company's willingness to use deceptively-obtained user data to target key competitors by discriminatorily denying them access to the "Facebook Platform."

170. The "Facebook Platform" allows third parties to develop products which work in conjunction with Facebook. Zuckerberg has described the "Facebook Platform's" purpose as "mak[ing] Facebook into something of an operating system so you can run full applications[.]"¹⁴² In order to access this "operating system," developers and third parties must send data to, and receive data from, Facebook using its application programming interfaces ("APIs").

171. In making its dominant "Platform" available to third parties, Facebook recognized that such access would be profitable to Facebook. Facebook, however, has selectively foregone those benefits and used discriminatory access to its social graph and pretextually enforced its "Platform" policies to prevent possible competitors from emerging, continuing to harm consumers at every turn. As Zuckerberg said regarding identified competitive threats: "I think the right solution here is to just be a lot stricter about enforcing our policies and identifying companies as competitors."¹⁴³

172. Facebook did exactly that, using supposed violations of its policies as a pretext to cut off social apps that had become too popular, like Vine, Stackla, Ark, and MessageMe. Facebook

¹⁴² David Kirkpatrick, *Facebook's plan to hook up the world*, CNN Money (May 29, 2007), available at <https://kl.link/3qrmFGT> (last accessed Apr. 15, 2021).

¹⁴³ House Report, *supra*, at 167.

1 cut off these social apps’ access to Facebook users’ data because Facebook was fearful that
 2 continued access would allow these apps to launch their own competing services that would
 3 challenge any one of Facebook’s ever-expanding cache of products.¹⁴⁴ As an example, Facebook
 4 penalized Ark, a third-party app that Facebook users could use in conjunction with Facebook, for
 5 the manner in which Ark accessed data on Facebook.¹⁴⁵ A former Facebook employee explained
 6 that in mid-2012: “[i]t seemed clear that leadership imposed [a] more severe punishment against
 7 Ark because Mr. Zuckerberg viewed Ark as competitive with Facebook, as Facebook was exploring
 8 an acquisition of Ark at the same time as it was being investigated for policy violations.”¹⁴⁶

9 173. By the end of 2011 and the beginning of 2012, Facebook executives debated a plan
 10 to prevent third-party developers from building their own competing social networks that might be
 11 capable of generating engagement and data independent of Facebook’s network. Social media
 12 applications, such as Line, WeChat, and Instagram were creating their own independent user bases
 13 and adding features that made them emerging competitive threats.

14 174. Facebook’s solution to address these potential competitors was a scheme to disrupt
 15 the growth of these applications by first attracting third-party app developers to build applications
 16 for Facebook’s “Platform” and then ultimately remove their access to the APIs, which removed
 17 those developers’ access to the functionality of Facebook’s social network as well as information
 18 about Facebook users’ friends and extended network, users’ interactions with each other, and users’
 19 newsfeed posts. This API access was the central value proposition of Facebook’s “Platform.” If
 20 developers built apps that enhanced the value of Facebook’s social network, they would in return
 21 receive the benefits of access to the functionality of Facebook’s social network, as well as to
 22 interconnections and interactions among Facebook’s users—Facebook’s social graph.

23 175. Facebook’s shut off of API access deprived app developers of access to the APIs
 24 that were most central to their applications, such as Facebook’s “Friends” and “Timeline” APIs, as
 25 well as other vital APIs, including those relating to messaging. Facebook’s identification of
 26

27 ¹⁴⁴ *Id.* at 166.

28 ¹⁴⁵ *Id.* at 169.

¹⁴⁶ *Id.*

1 competitive threats and removal of access to these APIs halted the growth of tens of thousands of
2 third-party applications that relied on these essential APIs and were, in Facebook’s view,
3 threatening Facebook’s monopolies by eroding the substantial barriers to entry that protected
4 Facebook’s business. Facebook’s scheme prevented competitive third-party applications from
5 buying consumer data from Facebook, either through its APIs or through its advertising network.
6 As a Facebook executive explained in 2012, Facebook would “not allow things which are at all
7 competitive to ‘buy’ this data from us.”

8 176. In May 2012, Zuckerberg decided to use the threat of shutting off potential
9 competitors’ access from Facebook’s “Platform” so that Facebook could extract more data. He
10 instructed executives to demand “reciprocity” agreements from major competitors that used
11 Facebook’s “Platform.” Facebook then began to block competitors from using its platform and
12 thereby obtaining access to Facebook’s data about consumers. Competitors such as Twitter,
13 Instagram, Pinterest, and Foursquare were required to hand over their most valuable asset—their
14 social data—to their rival Facebook in order to retain access to Facebook’s APIs and advertising
15 network.

16 177. Facebook planned to block competitors from using its “Platform,” thereby
17 preventing them from eroding the substantial barriers to entry and network effects that protected
18 Facebook’s market power. For the companies with social data that Facebook needed to further
19 extend its dominance, Facebook would coerce them into agreements to share their most valuable
20 social data with Facebook. If they refused, Facebook would blacklist them and take it from them
21 anyway with its own crawling software that would scrape their public-facing site for information.
22 What began as a negotiation strategy to extract social data from rivals became the foundation of
23 Facebook’s “Platform” strategy. For competitors that posed enough of a threat to create their own
24 rival network, Facebook required them to hand over the only leverage they had—the social data
25 they derived from their users’ engagement.

26 178. Facebook’s willingness to copy and penalize competitors through discriminatory
27 access to its social graph also made it easier for Facebook to acquire competitors at a reduced price.
28 For example, during negotiations to acquire Instagram between Zuckerberg and Kevin Systrom,

Instagram’s Chief Executive Officer, Zuckerberg tied Instagram’s continued access to Facebook “Platform” and Facebook’s social graph to Instagram’s response to Facebook’s acquisition offer:

At some point soon, you’ll need to figure out how you actually want to work with us. This can be an acquisition, through a close relationship with Open Graph, through an arms length relationship using our traditional APIs, or perhaps not at all . . . Of course, at the same time we’re developing our own photos strategy, so how we engage now will determine how much we’re partners vs. competitors down the line—and I’d like to make sure we decide that thoughtfully as well.¹⁴⁷

179. Similarly, in an earlier conversation between Systrom and Matt Cohler, an Instagram investor and former senior Facebook adviser, Systrom and Cohler discussed the possibility that Instagram’s response to Facebook’s acquisition efforts could affect Instagram’s access to Facebook “Platform” down the line.¹⁴⁸ In discussing how to engage with Zuckerberg regarding Facebook’s advances, Cohler cautioned: “we need to make it as hard as possible for fb to mess with our ability to get distribution on the platform[.]”¹⁴⁹

180. In 2015, Facebook cut off all public access to the Friends and News Feed APIs. Facebook had already extracted valuable social network data from dozens of competitors in the run-up to the announcement and ultimate removal of the APIs. This move allowed it to coerce incipient competitive threats to hand over their social network data. Facebook denied API access to thousands of potential competitors, and in the process ensured that its “Platform” would be the only viable “platform” upon which a third-party social media application could be built.

181. Even though it had eliminated public access to the Friends and News Feed APIs, Facebook strong-armed certain competitors into continuing to hand their data over to Facebook through agreements known as “Whitelist and Datasharing Agreements.”¹⁵⁰ Facebook demanded

¹⁴⁷ *Id.* at 164.

¹⁴⁸ Production of Facebook to H. Comm. on the Judiciary (Feb. 13, 2012) at FB-HJC-ACAL-00101440, available at <https://judiciary.house.gov/uploadedfiles/0010143800101441.pdf> (last accessed Apr. 15, 2021).

¹⁴⁹ *Id.*

¹⁵⁰ Facebook provided Whitelist and Data Sharing agreements to the dating apps Tinder and Hinge. To further entrench its social graph and gain even more access to data, it also secretly signed Whitelist and Data Sharing agreements with other third parties, including Netflix, Nissan, and Lyft. In total, dozens of third parties entered into such agreements with Facebook.

1 that the third-party developers it identified as competitive threats execute a standard form
 2 agreement, which Facebook referred to as a “Private Extended API Addendum.”¹⁵¹ These
 3 agreements “enable[d] Developer[s] to retrieve data or functionality relating to Facebook that is
 4 not generally available under Platform, which may include persistent authentication, photo upload,
 5 video upload, messaging and phonebook connectivity.”¹⁵² Importantly, a third-party developer’s
 6 “spending substantial sums with Facebook” was “a condition of maintaining preferential access to
 7 personal data” through Whitelist and Datasharing Agreements.¹⁵³

8 182. As part of this scheme, Facebook also mandated “reciprocity” from these third-party
 9 developers, “requiring apps that used data from Facebook . . . share . . . their data back to Facebook
 10 (with scant regard to users’ privacy).”¹⁵⁴ Indeed, Facebook’s reciprocity policies exponentially
 11 multiplied the effect of its deception of users regarding their privacy: “[b]y logging into an app
 12 such as Tinder, for instance, the user would not have realized they were giving away all their
 13 information on Facebook.”¹⁵⁵

14 183. Consistent with Facebook’s ploy to maintain its monopolistic grip on the Social
 15 Network and Social Media Markets by deceiving consumers about its privacy practices, Facebook’s
 16 Simon Cross marketed these changes to its third-party access policies as triumphs which bolstered
 17 the security of its users’ data. Facebook announced a new slogan, “‘People First’, because ‘if
 18 people don’t feel comfortable using Facebook and specifically logging in Facebook and using
 19 Facebook in apps, we don’t have a platform, we don’t have developers.’”¹⁵⁶ In reality, however,
 20 Facebook described these changes—and its marketing of these changes—as “the Switcheroo Plan”:
 21 “Facebook bundled in the decision to cut off third-party access to user data with other unrelated

22 ¹⁵¹ DCMS Report, *supra*, ¶ 85.

23 ¹⁵² *Id.*

24 ¹⁵³ *Id.*, ¶ 96.

25 ¹⁵⁴ *Id.*, ¶ 106.

26 ¹⁵⁵ *Id.*

27 ¹⁵⁶ Josh Constine, *Facebook Is Shutting Down Its API For Giving Your Friends’ Data to*
 28 *Apps*, TechCrunch (Apr. 28, 2015), available at <https://techcrunch.com/2015/04/28/facebook-api-shut-down/> (last accessed Apr. 15, 2021).

1 privacy updates, and explained it all under the new slogan ‘people first.’”¹⁵⁷ “The fact that user
 2 data would still be available to some third parties, as long as the companies gave Facebook enough
 3 money and didn’t pose a competitive threat, was conveniently elided.”¹⁵⁸

4 184. Absent these agreements and Facebook’s overall scheme to eliminate nascent
 5 competitors, other companies could have created their own social networks and social media
 6 applications. As the amount of user data was generated and monetized on these other networks and
 7 applications, the substantial barriers to entry in the Social Network and Social Media Markets
 8 would have eroded. But because Facebook could coercively demand all of the data generated on a
 9 competing “platform,” the Whitelist and Data Sharing Agreements ensured that competitive threats
 10 could not challenge Facebook’s stranglehold over the data, which Facebook obtained by leveraging
 11 its monopolies in the Social Network and Social Media Markets.

12 185. In all of its conduct surrounding potential acquisitions, Facebook intentionally
 13 surveilled, copied, acquired, and killed competitors with the specific intent, and result, of destroying
 14 competition. Facebook acquired and maintained its monopolies in the Social Network Market and
 15 the Social Media Market due to its predatory and anticompetitive conduct that went on during its
 16 string of acquisitions, with a specific intent to monopolize, and with a dangerous probability at the
 17 outset and, ultimately, its present day success in obtaining and maintaining its market power.

18 **Instagram**

19 186. Facebook used the undisclosed surveillance of its users to identify Instagram as a
 20 threat and ultimately to acquire the company. Instagram is a photo-sharing mobile application
 21 founded by Kevin Systrom, which allowed users to check in, post plans, and share photos. The
 22 photo sharing feature immediately became the app’s most popular feature.

23 187. Instagram launched on Apple’s mobile device operating system in 2010,
 24 immediately becoming the top free photo-sharing app on Apple’s App Store. On its very first day,
 25

26 ¹⁵⁷ Elena Botella, *Facebook Earns \$132.80 From Your Data per Year*, Slate (Nov. 15,
 27 2019), available at [https://slate.com/technology/2019/11/facebook-six4three-pikinis-lawsuit-](https://slate.com/technology/2019/11/facebook-six4three-pikinis-lawsuit-emails-data.html)
 28 [emails-data.html](https://slate.com/technology/2019/11/facebook-six4three-pikinis-lawsuit-emails-data.html) (last accessed Apr. 15, 2021).

¹⁵⁸ *Id.*

1 Instagram was downloaded 25,000 times. By December 2010, just several months after it had
2 launched, Instagram had been downloaded 1 million times.

3 188. By March 2012, Instagram enjoyed 27 million users. One month later, in April
4 2012, Instagram became available on Android devices. Just 10 days after its Android launch,
5 Instagram's overall user base jumped by 10 million, surpassing 40 million.¹⁵⁹ As a result, Instagram
6 was poised to receive additional funding based on a valuation of \$500 million.

7 189. Facebook recognized that Instagram posed a danger to Facebook's dominance.
8 Instagram's superior photo-sharing feature gave Instagram a hook to amass a large user base. Had
9 its user base continued to grow, and had it continued to add features, Instagram could have
10 threatened Facebook's stranglehold, not only on the Social Media Market, but also on the Social
11 Network Market as well. As such, Facebook obsessively tracked Instagram's rise, including
12 through intelligence that it received from surveilling Facebook users' behavior and that it obtained
13 from Onavo.¹⁶⁰

14 190. Both line employees and high-level executives at Facebook recognized Instagram
15 as a competitive threat. In an internal Facebook message, one engineer mused that "Instagram is
16 eating our lunch. We should've owned this space, but we're already losing quite badly."¹⁶¹ At an
17 internal meeting with Facebook employees, Zuckerberg put it bluntly: the "bad news is that
18 [Instagram is] growing really quickly, they have a lot of momentum, and it's going to be tough to
19 dislodge them."¹⁶²

22 ¹⁵⁹ Andrew Webster, *Instagram surpasses 40 million users ten days after Android launch*,
23 The Verge (Apr. 13, 2012), available at <https://www.theverge.com/2012/4/13/2946602/instagram-40-million-users> (last accessed Apr. 9, 2021).

24 ¹⁶⁰ Mike Swift, *Facebook's history with Onavo resonates for privacy experts worried about*
25 *Giphy purchase*, mlex Market Insight (June 23, 2020), available at
26 <https://mlexmarketinsight.com/insights-center/editors-picks/area-of-expertise/data-privacy-and-security/facebooks-history-with-onavo-resonates-for-privacy-experts-worried-about-giphy-purchase> (last accessed Apr. 15, 2021).

27 ¹⁶¹ House Report, *supra*, at 163.

28 ¹⁶² *Id.*

191. Consistent with its strategy of “copying” would-be competitors, Facebook initially attempted to create its own product that competed with Instagram. By June 2011, Facebook had begun developing its own photo-sharing app.¹⁶³ One Facebook employee referred to Facebook’s anticipated photo-sharing app as “an Instagram clone.”¹⁶⁴ Facebook subsequently released Facebook Camera, a standalone app allowing users to shoot, filter, and share photos from their mobile devices.¹⁶⁵

192. In addition to “cloning” Instagram, Facebook determined there was another way to hedge its bets, protect its monopoly, and neutralize the competitive threat of Instagram: simply buying Instagram outright. Accordingly, after direct talks with Mark Zuckerberg, Facebook offered to purchase Instagram for \$1 billion in April 2012.

193. In addition to the \$1 billion price tag, another consideration motivated Instagram’s evaluation of Facebook’s acquisition offer: Facebook’s aggressive and anticompetitive threats, which Facebook was safe to make due to its status as a monopolist. During negotiations between Facebook and Instagram, Zuckerberg warned Kevin Systrom, Instagram’s Chief Executive Officer, that “[a]t some point soon, you’ll need to figure out how you actually want to work with us. . . . [H]ow we engage now will determine how much we’re partners vs. competitors down the line—and I’d like to make sure we decide that thoughtfully as well.”¹⁶⁶ In a separate communication with Matt Cohler—an Instagram investor and Facebook’s former Vice President of Product Management—Systrom inquired whether Zuckerberg “will go into destroy mode if I say no” to Facebook’s acquisition offer.¹⁶⁷ Cohler responded that Zuckerberg would “probably” go into

¹⁶³ MG Siegler, *Behold: Facebook’s Secret Photo Sharing App*, TechCrunch (June 15, 2015), available at https://techcrunch.com/2011/06/15/facebook-photo-sharing-app/?_ga=2.238331010.340941203.1606233329-687565188.1605321310 (last accessed Apr. 5, 2021).

¹⁶⁴ House Report, *supra*, at 163.

¹⁶⁵ Josh Constine, *FB Launches Facebook Camera – An Instagram-Style Photo Filtering, Sharing, Viewing iOS App*, TechCrunch (May 24, 2012), available at <https://techcrunch.com/2012/05/24/facebook-camera/> (last accessed Apr. 15, 2021).

¹⁶⁶ House Report, *supra*, at 163–64.

¹⁶⁷ Production of Facebook to H. Comm. on the Judiciary (Feb. 13, 2012) at FB-HJC-ACAL-00101438, available at <https://judiciary.house.gov/uploadedfiles/0010143800101441.pdf> (last accessed Apr. 15, 2021).

1 “destroy mode” and “conclude that it’s best to crush Instagram[.]”¹⁶⁸ Cohler further lamented that
 2 “I don’t think we’ll ever escape the wrath of [M]ark” Zuckerberg.¹⁶⁹

3 194. Clearly crushed into submission and fearful of Facebook’s “wrath,” Instagram
 4 acceded to Facebook’s acquisition demand. Facebook consummated the deal immediately prior to
 5 its IPO.

6 Snapchat

7 195. Following its acquisition of Instagram, Facebook excluded third-party apps that
 8 provided photo and video sharing functionality from Facebook’s “Platform.” If an image sharing
 9 or video app contained an important feature, Facebook simply cloned it, thus paving the way for
 10 excluding a competitive rival from its “Platform,” while simultaneously taking away that rival’s
 11 share of users. And, high-level Facebook executives were acutely aware of this strategy.¹⁷⁰

12 196. For example, by 2012, the photo-sharing app Snapchat had grown in popularity
 13 among consumers. Founded by Evan Spiegel, Snapchat allows users on that application to send
 14 each other communications—including text, photos, and videos—which appear only for a fixed
 15 period of time and then disappear.¹⁷¹ Drawn by Snapchat’s privacy appeal, users began to flock to
 16 Snapchat.

17 197. Facing a competitive threat from Snapchat, Facebook engaged in its usual “copy,
 18 acquire, kill” strategy in an attempt to annihilate Snapchat. To formulate that strategy, Facebook
 19 relied on data it obtained from Onavo.¹⁷²

22 ¹⁶⁸ *Id.* at FB-HJC-ACAL-00101438–39.

23 ¹⁶⁹ *Id.* at FB-HJC-ACAL-00101440.

24 ¹⁷⁰ Executives such as Zuckerberg, Sheryl Sandberg (Facebook’s Chief Operating Officer),
 25 and Sam Lessin (Facebook’s Product Management Director), expressly endorsed “cloning” other
 competing applications’ popular features. *See* House Report, *supra*, at 163.

26 ¹⁷¹ Srinivasan, *supra*, at 53.

27 ¹⁷² Karissa Bell, “*Highly confidential*” documents reveal Facebook used VPN app to track
 28 competitors, Mashable (Dec. 5, 2018), available at: <https://mashable.com/article/facebook-used-onavo-vpn-data-to-watch-snapchat-and-whatsapp/> (last accessed Apr. 15, 2021).

198. In December 2012, Facebook launched “Poke,” a standalone app designed to allow users to send photos, videos, or Facebook messages to each other that expire after a few seconds.¹⁷³ But to Facebook, the possibility of competing with Snapchat on the merits provided insufficient guarantee that Facebook’s monopoly position would be secure. So, mere days before Facebook launched Poke, Zuckerberg met with Spiegel, Snapchat’s founder, in Los Angeles.¹⁷⁴ During the meeting, Zuckerberg described Facebook’s soon-to-be-released Poke app to Spiegel. Spiegel has described Zuckerberg’s representations during the meeting as follows: “It was basically like, ‘We’re going to crush you.’”¹⁷⁵

199. After the meeting and following Facebook’s launch of Poke, Facebook made additional overtures to Snapchat in an attempt to cement its top-of-the-ladder status.¹⁷⁶ Facebook ultimately offered \$3 billion to acquire Snapchat. Facebook’s \$3 billion offer made clear that Facebook was willing to pay a premium over Snapchat’s then-existing market value for the added security of neutralizing a possible threat to Facebook’s market dominance.

200. Snapchat rejected Facebook’s offer, and Facebook responded by copying *even more* of Snapchat’s features that are popular with consumers. For example, Snapchat’s “Stories” feature allows Snapchat users to post a collection of images and video in a rapid string that other Snapchat users may view for 24 hours. In 2016, Facebook (through Instagram) launched its own feature—also called “Stories”—which is “nearly identical” to Snapchat’s version.¹⁷⁷ By April 2017,

¹⁷³ Josh Constone, *Facebook Launches Snapchat Competitor ‘Poke’, An iOS App for Sending Expiring Text, Photos, And Videos*, TechCrunch (Dec. 21, 2012), available at: <https://techcrunch.com/2012/12/21/facebook-poke-app/> (last accessed Apr. 15, 2021).

¹⁷⁴ J.J. Colao, *The Inside Story Of Snapchat: The World’s Hottest App Or A \$3 Billion Disappearing Act?*, Forbes (Jan. 20, 2014), available at https://www.forbes.com/sites/jjcolao/2014/01/06/the-inside-story-of-snapchat-the-worlds-hottest-app-or-a-3-billion-disappearing-act/?utm_campaign=forbestwittersf&utm_medium%0b=social&utm_source=twitter&sh=3e058aae67d2 (last accessed Apr. 15, 2021).

¹⁷⁵ *Id.*

¹⁷⁶ *Id.*

¹⁷⁷ Casey Newton, *Instagram’s new stories are a near-perfect copy of Snapchat stories*, The Verge (Aug. 2, 2016), available at <https://www.theverge.com/2016/8/2/12348354/instagram-stories-announced-snapchat-kevin-system-interview> (last accessed Apr. 15, 2021).

Facebook’s “Stories” feature on Instagram had become more popular than Snapchat’s version, crippling one of Facebook’s largest rivals.¹⁷⁸

WhatsApp

201. Facebook’s acquisition of WhatsApp followed a similar pattern. WhatsApp began as a mobile application that displayed user statuses in an address book on a smartphone. However, WhatsApp exploded in popularity when Apple introduced “push notifications” for the iPhone, allowing developers to ping app users even when they weren’t using the app. This feature became a form of instant messaging, enabling users to broadcast messages to connections within a user’s social network, which was built from their phone’s contact list. Because WhatsApp used the mobile phone’s internet connection rather than text messages over the phone’s cellular connection, the app allowed users to avoid text messaging fees entirely. WhatsApp’s ability to send messages to any user with a phone using the internet was its most sought-after feature.

202. As WhatsApp’s popularity began to rise in the early 2010s, Facebook harvested user engagement data from Facebook’s Onavo spyware in order to carefully track WhatsApp. The data reported that WhatsApp was rivaling Facebook’s own Messenger product, and held third place in terms of user reach among mobile messenger apps for iPhone in the U.S. as of April 2013. Facebook used Onavo’s data to track messages sent through WhatsApp, which more than doubled messages on Facebook’s own mobile product. This same Onavo data showed massive engagement among WhatsApp users, placing it in fifth place behind Facebook’s own core product; Facebook’s newly acquired Instagram; Twitter; Foursquare; and Snapchat. WhatsApp threatened Facebook’s business—including the barriers to entry and network effects protecting Facebook’s dominance—and because of Onavo, Facebook knew that WhatsApp was a direct threat to Facebook’s monopoly power.

203. Facebook then sought to remove WhatsApp as a competitor in order to ensure that Facebook retained its monopoly power in the Social Network and Social Media Markets. Facebook used the insights it had gained from Onavo’s data surveillance technology to purchase WhatsApp

¹⁷⁸ Kaya Yurieff, *Instagram’s Snapchat clone is more popular than Snapchat*, CNN Business (Apr. 13, 2017), available at <https://money.cnn.com/2017/04/13/technology/instagram-stories-snapchat/index.html> (last accessed Apr. 15, 2021).

1 in 2014 for close to \$22 billion, well above its initial bid of \$16 billion. The transaction made no
 2 economic sense for Facebook, other than foreclosing competition in the Social Media and Social
 3 Network Markets and protecting Facebook’s monopoly power. WhatsApp’s revenues were a
 4 meager \$10.2 million in 2013. Its six-month revenue for the first half of 2014 totaled \$15.9 million,
 5 and the company had incurred a staggering net loss of \$232 million in that same period. Facebook
 6 had paid twenty billion dollars—thousands of times WhatsApp’s revenues—to acquire a money-
 7 losing company that created software functionality Facebook itself already had as part of its own
 8 products, and could easily build from scratch for a fraction of the cost of the acquisition.

9 **Other Examples of Facebook’s “Copy, Acquire, Kill” Strategy**

10 204. In addition to the examples described herein, Facebook has employed its “copy,
 11 acquire, kill” strategy against other would-be competitors, and the extent to which it did so based
 12 on deceptively-obtained user data only first began to become known recently. For example, data
 13 that Facebook collected from Onavo reportedly put “Houseparty”—a social network that referred
 14 to itself as “the internet’s living room”—in Facebook’s crosshairs.¹⁷⁹

15 205. After Houseparty turned down an acquisition offer from Facebook, Facebook
 16 announced that its Messenger app would become a “virtual living room.” Houseparty’s active user
 17 base fell by half between 2017 and 2018.

18 206. As another example, Facebook acquired Giphy for \$400 million in May 2020.
 19 Although Giphy’s primary function is to allow users to share GIFs¹⁸⁰ online and through messaging
 20 apps, the transaction will also give Facebook competitive insights into other messaging apps. One
 21 commenter said, “While you may successfully block trackers like the Facebook ad pixel following
 22
 23
 24

25 ¹⁷⁹ Rachel Sandler, *People are furious about Onavo, a Facebook-owned VPN app that sends*
 26 *your app usage habits back to Facebook*, Business Insider (Feb. 14, 2018), available at
 27 [https://www.businessinsider.com/what-is-facebooks-onavo-protect-virtual-private-network-app-](https://www.businessinsider.com/what-is-facebooks-onavo-protect-virtual-private-network-app-2018-2?r=US&IR=T)
 28 [2018-2?r=US&IR=T](https://www.businessinsider.com/what-is-facebooks-onavo-protect-virtual-private-network-app-2018-2?r=US&IR=T) (last accessed March 29, 2021).

¹⁸⁰ A “GIF” is a compilation of still images, akin to a flipbook, played in sequence to create a short animated sequence.

1 you around online, or even delete your Facebook account, the majority of us wouldn't suspect we're
2 being monitored when we're sending funny images to friends.”¹⁸¹

3 207. In addition, Facebook has sometimes acquired companies without the goal of
4 incorporating them into its own business, but rather, simply to eliminate the competitor, a practice
5 referred to as “catch and kill.” For example, Facebook acquired “tbh”—an anonymous social media
6 app—in October 2017. It then shut the app down less than a year later, having made little effort to
7 maintain the application.¹⁸²

8 208. Facebook's acquisition conduct is part of an ongoing attempt to entrench its market
9 power in the Social Network and Social Media Markets. Facebook's strategy was made possible
10 due to the social data that Facebook obtained as it acquired its monopolies. And, Facebook has
11 used that data in order to copy, acquire, or kill competitors, instead of competing with them by
12 providing enhanced data privacy protections to consumers.

13 **G. Facebook's Use of Onavo Comes to Light.**

14 209. Ultimately, the world learned the truth about the extent of commercial surveillance
15 that technology like Onavo's made possible for Facebook. In August 2018, Apple removed Onavo
16 from its app store following reporting that Facebook was using the app to track users and other
17 apps. Apple ejected Facebook's Onavo app from its marketplace because it violated Apple's rules
18 prohibiting apps from using data in ways far beyond what is required to run the app and provide
19 advertising. In other words, because Onavo Protect was leveraging far more data than any VPN
20 could conceivably need, it was clear that the true purpose of the app was to spy on Onavo users,
21 and Apple would not allow it. An Apple spokesperson said the company intended to make “it
22 explicitly clear that apps should not collect information about which other apps are installed on a
23
24
25

26 ¹⁸¹ Owen Williams, *How Facebook Could Use Giphy to Collect Your Data*, ONEZERO,
27 May 15, 2020, available at <https://kl.link/34AW951> (last accessed Apr. 15, 2021).

28 ¹⁸² See Kaya Yurieff, *Facebook Shuttters the Teen App it Just Bought*, CNN Business (July
3, 2018), available at <https://kl.link/37G6HBH> (last accessed Apr. 15, 2021).

1 user's device for the purposes of analytics or advertising/marketing and must make it clear what
2 user data will be collected and how it will be used.”¹⁸³

3 210. The amount of commercial surveillance that Onavo's technology enabled was jaw-
4 dropping. Facebook's Onavo Protect app reported on users' activities whether their screens were
5 on or off, whether they used WiFi or cellular data, and even when the VPN was turned off. There
6 was simply no rational relationship between the data collected and the purported purpose of the
7 application. Put simply, a VPN that collected data even when the VPN was off was an obvious
8 subterfuge for spying on users and user behavior.

9 211. Facebook tried to circumvent Apple's ban by repackaging its Onavo spyware as a
10 Facebook Research VPN app. Facebook sidestepped the App Store by rewarding teenagers and
11 adults when they downloaded the Research app and gave it root—superuser—access to network
12 traffic on their mobile devices. Facebook has been leveraging its Onavo code in similar ways since
13 at least 2016, administering the program under the codename “Project Atlas”—a name suited to its
14 goal of surveilling app usage on mobile devices in real time.

15 212. When the news broke in January 2019 that Facebook's Research apps were
16 repackaged Onavo apps designed to spy on users, Facebook immediately withdrew the programs
17 from the Apple App store. Apple again concluded that Facebook had tried to violate its policies by
18 obtaining a level of administrative privileges on an iPhone or iPad that would have been designed
19 for the internal IT department of the device user's employer.

20 213. In addition to Onavo's Protect app, Facebook has attempted to deploy its
21 surveillance software as other forms of utility applications that require extensive or privileged
22 access to mobile devices. For example, Facebook released the Onavo Bolt app, which Facebook
23 represented would allow a user to block unauthorized access to particular apps on the user's phone,
24 unless a particular passcode, fingerprint, or other information was provided. In reality, however,
25 Onavo Bolt covertly surveilled users and sent Facebook the results. Facebook also shut that app
26

27 ¹⁸³ Ari Levy, *Apple removes Facebook's Onavo security app from the App Store*, CNBC
28 (Aug. 22, 2018), available at <https://www.cnbc.com/2018/08/22/apple-removes-facebook-onavo-app-from-app-store.html> (last accessed Apr. 22, 2021).

down the very day that its surveillance functionality was discovered. The Onavo Bolt app had been installed approximately 10 million times.

H. Facebook’s Anticompetitive Practices Have Harmed and Continue to Harm Competition in the Social Network and Social Media Markets.

214. Facebook’s anticompetitive practices described above have harmed and continue to harm competition in the Social Network and Social Media Markets in the United States.¹⁸⁴

215. Facebook is dangerously close to obtaining, or has obtained, monopoly power in the Social Network and Social Media Markets in the United States, and it has wielded that power to anticompetitively foreclose competition.

216. Facebook’s deception of consumers has harmed, and continues to harm, competition. In many markets, the advantage of consumer deception quickly dissolves once the deception is uncovered. But the direct and indirect network effects inherent in the Social Network and Social Media Markets create markets with strong network effects and high barriers to entry. Because of unduly high switching costs, users cannot simply switch to a competitor once the dominant player’s deception is exposed, even though they wanted to do so, as evidenced by the “#DeleteFacebook” movement after the revelations regarding Cambridge Analytica in 2018.

217. Facebook’s deception about its lack of privacy protections acted as a welcome sign, inducing a ground swell of users to join Facebook because of Facebook’s avowed privacy appeal. But once a critical mass of users, continually expanding due to strong network effects obtained through its deception, joined Facebook at the expense of its competitors, Facebook slammed the

¹⁸⁴ As a former Assistant Attorney General for the DOJ’s Antitrust Division has explained, “[i]t is well-settled . . . that competition has price and non-price dimensions.” Makan Delrahim, Assistant Attorney General, U.S. Dep’t of Justice Antitrust Div., Remarks for the Antitrust New Frontiers Conference (June 11, 2019), available at: <https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-antitrust-new-frontiers>. Similarly, when asked whether “when . . . conducting competition analysis in the tech industry, non-price factors should be considered,” Facebook CEO Mark Zuckerberg testified before the United States House of Representatives Committee on Energy & Commerce that “the law already includes quality of products in addition to price.” *Social Media’s Role in Promoting Extremism and Misinformation*, 117th Cong. (Mar. 25, 2021), video available at <https://energycommerce.house.gov/committee-activity/hearings/hearing-on-disinformation-nation-social-medias-role-in-promoting> (starting at 4:31:40).

1 door shut. Because of high switching costs—including the possibility of losing contact with
2 friends, family and acquaintances, an inability to access data that Facebook users have spent years
3 or more inputting into Facebook, and the time and opportunity cost of starting over with a
4 competitor—and the lack of viable alternatives as a result of Facebook’s deception, consumers are
5 now trapped. As a result, Facebook has cheated its way to the finish line in the race for dominance
6 without being the best competitor. Instead of providing consumers a way out, such as alternatives
7 to Facebook, the Social Network and Social Media Markets help to lock in Facebook’s unfair
8 advantage.

9 218. Facebook’s acquisition conduct also has harmed, and continues to harm,
10 competition. Facebook built and maintained its monopolies over the Social Network and Social
11 Media Markets by exploiting deceptively-obtained user data to target competitive threats, which
12 Facebook then proceeded to acquire, copy, or kill. Facebook tracked its users across the internet,
13 often without permission, to identify companies that might threaten its monopoly. Facebook then
14 used a pattern of discriminatory data access to destroy potential competitors or force them to sell
15 at a discount. Facebook’s policy of shutting off these firms’ access to Facebook’s valuable user
16 data if Facebook declared them competitive threats stymied the emergence of competing social
17 networks and social media applications. Put simply, Facebook used its data advantage not to run
18 faster, but to kneecap the competition. That approach is not surprising given the win-at-all-costs
19 culture at Facebook.

20 219. Facebook’s two-pronged anticompetitive strategy harmed competition in the Social
21 Network and Social Media Markets. As detailed herein, Facebook’s strategies made it nearly
22 impossible for competitors—both nascent and established—to challenge Facebook’s monopoly by
23 competing with Facebook on data privacy protections or by building a higher quality social
24 network.

25 220. But for Facebook’s anticompetitive practices, consumers would have had more
26 options in the Social Network and Social Media Markets for accessing content and connecting with
27 other users. Those companies would have created social networks and social media applications
28 that competed with Facebook on the merits of data privacy protections and social network and

1 social media application quality, without being dependent on Facebook for comprehensive data.
 2 Because Facebook anticompetitively restrained competition in its efforts to acquire and obtain
 3 social media and social network monopolies, competition along the dimensions of user privacy and
 4 product quality was foreclosed. Ultimately, consumers suffered, and continue to suffer, as a result
 5 of Facebook's wantonly anticompetitive conduct.

6 **I. Facebook's Anticompetitive Conduct Has Directly and Quantifiably Damaged**
 7 **Consumers.**

8 221. Facebook's anticompetitive practices described herein have harmed, and continue
 9 to harm, consumers in the Social Network and Social Media Markets in the United States.

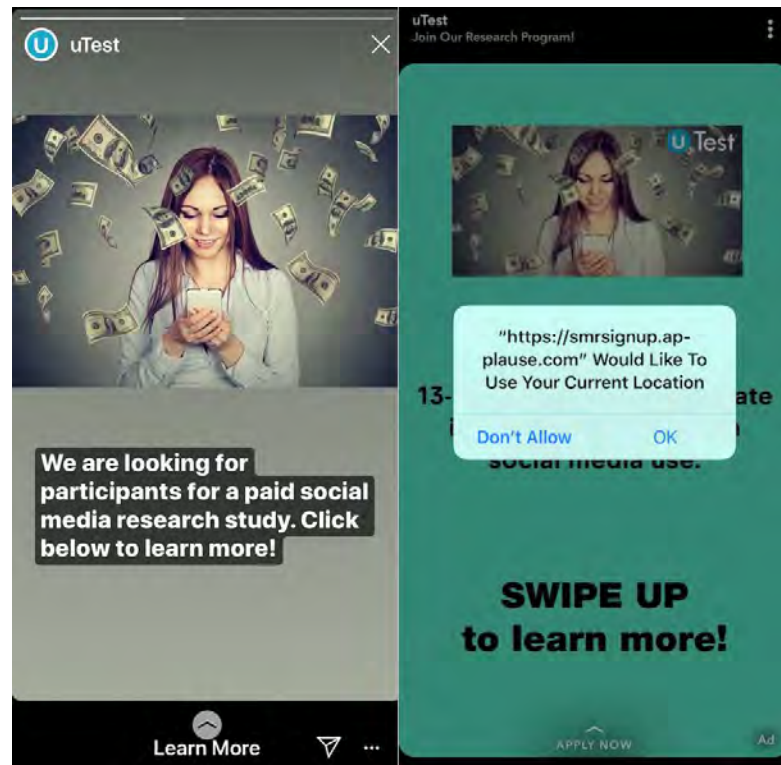
10 222. Facebook's anticompetitive foreclosure of competition has harmed consumers in
 11 many ways. When using Facebook's products, consumers agree to give up things of material
 12 value: personal information and attention. Facebook then sells for money, measurable in
 13 quantifiable units, its users' information and attention to third parties, including advertisers. But
 14 for Facebook's anticompetitive conduct, which has substantially reduced, if not eliminated
 15 competition, consumers would have had more choices in the Social Network and Social Media
 16 Markets, instead of the few, if any, they have today.

17 223. Vigorous competition would have benefitted consumers by requiring social
 18 networks and social media applications to employ those business models which best attract and
 19 retain users. When consumers agree to use Microsoft's "Bing" search engine and allow Microsoft
 20 to collect their data, Microsoft, for example, compensates consumers with items of monetary
 21 value.¹⁸⁵ Similarly, users who agree to provide their web browsing history to the Nielsen

22
 23
 24
 25
 26
 27 ¹⁸⁵ Lisa Marie Segarra, *Microsoft Will Pay You to Use Bing Instead of Google*, Fortune
 28 (June 3, 2017), available at <https://fortune.com/2017/06/03/microsoft-pay-use-bing-google/> (last
 accessed Mar. 29, 2021).

Corporation's Computer and Mobile Panel can receive \$50.00 a year.¹⁸⁶ Honeygain—a service that allows users to share their internet access data—compensates users up to \$19.00 a month.¹⁸⁷

224. Between 2016 and 2019—pursuant to its secret “Project Atlas”—Facebook itself paid users between the ages of 13 and 35 up to \$20.00 per month in return for access to those users' emails, private messages in social media apps, photos and videos, web browsing and search activity, and even location information.¹⁸⁸ Facebook cloaked its involvement by naming the app “Research” and advertising it through services that did not carry the Facebook moniker, including BetaBound, uTest, and Applause.¹⁸⁹ These ads prominently advised that participants would be compensated monetarily for their data:



¹⁸⁶ Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html> (last accessed Mar. 29, 2021).

¹⁸⁷ Honeygain, *How Our PayPal Payouts Are Done? Step by Step Instructions* (Dec. 17, 2019), available at <https://www.blog.honeygain.com/post/paypal-payouts-step-by-step-instructions> (last accessed March 29, 2021).

¹⁸⁸ Josh Constine, *Facebook pays teens to install VPN that spies on them*, TechCrunch (Jan. 29, 2019), available at <https://techcrunch.com/2019/01/29/facebook-project-atlas/> (last accessed Apr. 1, 2021).

¹⁸⁹ *Id.*

225. Absent Facebook’s anticompetitive conduct, Facebook would have had to provide consumers increased incremental value in return for consumers’ data. Otherwise, consumers would have given their data and attention to other social networks and social media applications, which would have provided consumers increased incremental value. Consumers would have received the fair market value for their data and attention.¹⁹⁰ That value was artificially decreased by Facebook’s anticompetitive conduct.

226. Absent Facebook’s anticompetitive conduct, which has substantially reduced, if not eliminated, competition, consumers would have benefitted from more robust competition in terms of non-price attributes such as data privacy practices and social network and social media application quality. Indeed, more robust competition would have benefitted consumers with increased innovation (including the development of superior product features) and increased consumer choice (including the ability to select a social network or social media application which offers consumers services that more closely align with the consumers’ preferences, such as with respect to the content displayed, quantity and quality of advertising, and options regarding data collection and usage practices). Consumers could have benefitted from Facebook’s social network and social media offerings without having to surrender as much personal data to Facebook and other third parties that use Facebook for app development or targeted advertising.¹⁹¹ Similarly, consumers could have benefitted from competition that would have resulted in Facebook or its alternatives offering higher-quality services, such as lower ad loads, interoperability between applications, and portability of users’ data. In the absence of this competition, many consumers

¹⁹⁰ Facebook indisputably recognizes that its users’ data has monetary value. In addition to secretly paying users who shared information outside of Facebook, Instagram, and WhatsApp as part of “Project Atlas,” Facebook, in 2019, for example, touted that its ARPU was over \$41.00 per user in the United States and Canada. And, in the aftermath of its IPO, Facebook executives openly discussed a “Data for \$” plan, explaining “we are wanting to put a \$ amount on data and a \$ amount on distribution.” *See* Goodwin, *supra*.

¹⁹¹ As FTC Commissioner Rohit Chopra explained in his testimony before the House Antitrust Subcommittee—with respect to Facebook in particular—“changes to terms of service hidden in the fine print where they can collect more and more data and unilaterally impose these terms, that is a price hike. We are paying with our data, that valuable data[.]” *Online Platforms and Market Power, Part 3: The Role of Data and Privacy in Competition*, 116th Cong. (Oct. 18, 2020), transcript available at <https://www.congress.gov/116/chrg/CHRG-116hhrg39840/CHRG-116hhrg39840.pdf> (page 115).

1 trapped in Facebook's social network and social media offerings have reduced their use of these
2 products.

3 227. If Facebook had disclosed the scope of the data it collected and the level of fine-
4 grained targeted marketing that it enabled, consumers would have benefitted from competition in
5 the Social Network and Social Media Markets, resulting in a better Facebook or better alternatives
6 and lower consumer costs in the form of information and attention. Instead, Facebook has
7 artificially stifled innovation, thrusting on consumers a product of reduced-quality and leaving
8 consumers with no meaningful alternative.

9 228. If Facebook had not used its social network and social media monopolies to target
10 its competition for destruction, consumers would have benefitted from more competition, and hence
11 more options and lower costs, in the Social Network and Social Media Markets. As elected officials
12 have recognized, absent Facebook's anticompetitive acquisition strategy, Facebook would have
13 had to compete on privacy issues, benefiting consumers.¹⁹²



Rep. Ro Khanna
@RepRoKhanna

Replying to @RepRoKhanna

2/2 -- Imagine how different the world would be if
Facebook had to compete with Instagram and
WhatsApp. That would have encouraged real
competition that would have promoted privacy and
benefitted consumers.

12:28 PM · Jan 25, 2019 · Twitter Web Client

27 Retweets 1 Quote Tweet 86 Likes

22 229. Because Facebook engaged in the anticompetitive practices described above,
23 consumers suffered substantial, cognizable, and quantifiable economic harm. Unless these acts are
24 enjoined, consumers will continue to suffer harm caused by Facebook's anticompetitive practices.

27 ¹⁹² United States Representative Ro Khanna, Twitter (Jan. 25, 2019), available at
28 <https://twitter.com/reprokhanna/status/1088850988218413058?lang=en> (last accessed Apr. 15,
2021).

V. STATUTE OF LIMITATIONS

A. Accrual of Claim

230. Plaintiffs did not discover the existence of the anticompetitive acts alleged herein until, at the earliest, March 17, 2018. As the House Antitrust Subcommittee recently explained, “[t]o the extent that consumers are aware of data collection practices, it is often in the wake of scandals involving large-scale data breaches or privacy incidents such as Cambridge Analytica.”¹⁹³

231. It was not until the media uncovered the details of the Cambridge Analytica scandal on March 17, 2018, that consumers began to discover Facebook’s anticompetitive practices that harmed consumers and that would have enabled consumers to raise the claims presented in this action. Indeed, the U.K. House of Commons’ Digital, Culture, Media and Sport Committee has specifically recognized that prior to at least, and no earlier than, March 2018, “Facebook users had *no idea* that their data was able to be accessed by developers unknown to them, despite the fact that they had set privacy settings, specifically disallowing the practice.”¹⁹⁴

232. Similarly, it was not until the media revealed the details of Apple’s ban of Onavo on August 22, 2018, that consumers learned of the additional facts regarding Facebook’s anticompetitive practices necessary for consumers to raise the claims presented in this action. Importantly, the Australian Competition and Consumer Commission—which has launched its own action against Facebook arising out of its deceptive use of Onavo—has asserted that, generally, “nowhere on the Onavo Protect website, the Apple App Store, the Google Play Store, or in the advertising for Onavo Protect did Facebook or Onavo disclose to consumers . . . that Onavo Protect would not protect and keep secret users’ personal activity data, or that Facebook or Onavo would use personal activity data collected from users for the commercial benefit of Facebook or Onavo.”¹⁹⁵

¹⁹³ House Report, *supra*, at 54.

¹⁹⁴ DCMS Report, *supra*, ¶ 75 (emphasis added).

¹⁹⁵ ACCC Complaint, *supra*, ¶ 8.

B. Equitable Tolling

233. Nor could plaintiffs have discovered, through the exercise of reasonable diligence, the existence of the anticompetitive acts alleged herein until, at the earliest, March 2018. Facebook did not adequately disclose its deception, nor did its privacy policies themselves make clear to consumers the scope of data it collected, the third parties who could access this data, and how this data could be used. Facebook’s privacy policies are dense and opaque.¹⁹⁶ Tellingly, Richard Allan—Facebook’s then-Vice President of Policy Solutions—conceded, in testimony to the U.K. House of Commons’ Digital, Culture, Media and Sport Committee, that “there are very valid questions about how well people understand [Facebook’s privacy] controls and whether they are too complex.”¹⁹⁷

234. Firms like Facebook that collect vast amounts of data from consumers often further obfuscate their data privacy policies to make them even more difficult for consumers to understand. Indeed, “these policies tell you very little about the data these websites have on you. And that’s the point. . . . They know that if they tell people every single way they’re collecting information and using it, then most users will share less information, which would mean less money for them.”¹⁹⁸

235. Accordingly, as the House Antitrust Subcommittee has recognized, “nuances in privacy terms are relegated to investigative journalists to discover and explain.”¹⁹⁹ The subsequent investigative reporting that brought to light Facebook’s systematic deception and commercial surveillance was not made public until, at the earliest, March 17, 2018, following the Cambridge Analytica scandal.

236. As such, the statute of limitations should be equitably tolled to at least March 2018. Accordingly, all of the anticompetitive conduct described in this complaint presents timely claims,

¹⁹⁶ House Report, *supra*, at 54.

¹⁹⁷ DCMS Report, *supra*, ¶ 82 (emphasis added).

¹⁹⁸ Marcus Moretti and Michael Naughton, *Why Privacy Policies Are So Inscrutable*, The Atlantic (Sept. 5, 2014), available at <https://www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615/> (last accessed Apr. 1, 2021).

¹⁹⁹ House Report, *supra*, at 54.

including Facebook’s deception and acquisition conduct going back to before it achieved its social network and social media monopolies.

C. Fraudulent Concealment

237. Facebook fraudulently concealed its deceptive practices and commercial surveillance efforts, including the extent of its data privacy practices and anticompetitive acquisition strategy. As a result, Plaintiffs and Class members were unaware of Facebook’s unlawful conduct alleged herein.

238. Facebook affirmatively and fraudulently concealed its unlawful conduct by, *inter alia*, publicly misrepresenting, before and after its 2011 settlement with the FTC—which “barred [Facebook] from making misrepresentations about the privacy or security of consumers’ personal information”—that it was protecting users’ privacy. Examples of such public statements include:

a) Mark Zuckerberg’s September 8, 2006 statement posted on Facebook, representing that “**we have built extensive privacy settings – to give you even more control** over who you share your information with”; apologizing that Facebook’s privacy mishap regarding its News Feed feature “**was a big mistake on our part, and I’m sorry for it**”; and explaining that “apologizing isn’t enough. I wanted to make sure we did something about it, and quickly. So **we have been coding nonstop** for two days **to get you better privacy controls.**”²⁰⁰

b) Mark Zuckerberg’s December 6, 2007 statement, posted on Facebook’s Newsroom, explaining that Facebook intended that its Beacon feature “would give people an easy and controlled way to share more . . . information with their friends”; acknowledging that “[i]t took us too long after people started contacting us to change the product . . . [i]nstead of acting quickly, we took too long to decide on the right solution”; and reassuring that while “I’m not proud of the way we’ve handled this situation,” “**I know we can do better.**”²⁰¹

²⁰⁰ Mark Zuckerberg, *An Open Letter from Mark Zuckerberg*, Facebook (Sept. 8, 2006), available at <https://www.facebook.com/notes/facebook/an-open-letter-from-mark-zuckerberg/2208562130/> (last accessed Apr. 18, 2021) (emphases added).

²⁰¹ Mark Zuckerberg, *Announcement: Facebook Users Can Now Opt-Out of Beacon Feature*, Facebook Newsroom (Dec. 6, 2007), available at <https://about.fb.com/news/2007/12/announcement-facebook-users-can-now-opt-out-of-beacon-feature/> (last accessed Apr. 20, 2021) (emphasis added).

c) Facebook’s May 26, 2010 statement posted on its Newsroom, indicating that Facebook “will give the more than 400 million people who use Facebook the power to **control exactly who can see** the information and content they share”; that “People have control over how their information is shared”; that “**Facebook does not share personal information with people or services users don’t want**”; that “Facebook does not give advertisers access to people’s personal information”; and that “**Facebook does not sell any of people’s information to anyone.**”²⁰²

d) Mark Zuckerberg’s May 27, 2010 statement on NPR that “There’s this false rumor that’s been going around which says that **we’re sharing private information with applications and it’s just not true.**”²⁰³

e) Mark Zuckerberg’s November 29, 2011 statement, posted on Facebook’s Newsroom, indicating that “I founded Facebook on the idea that people want to share and connect with people in their lives, but to do this **everyone needs complete control over who they share with at all times.**”²⁰⁴

f) Mark Zuckerberg’s November 29, 2011 statement, posted on Facebook’s Newsroom, indicating that Facebook’s settlement with the FTC “means we’re making a clear and formal long-term **commitment to** do the things we’ve always tried to do and planned to keep doing – **giving you tools to control who can see your information** and then **making sure only those people you intend can see it.**”²⁰⁵

²⁰² Facebook, *Facebook Redesigns Privacy*, Facebook Newsroom (May 26, 2010), available at <https://about.fb.com/news/2010/05/facebook-redesigns-privacy/> (last accessed Apr. 1, 2021) (emphases added).

²⁰³ Mark Memmott, *Facebook’s Zuckerberg Argues Against Making ‘Privacy’ Your ‘Default Setting’*, SCPR (May 27, 2010), available at: <https://www.scpr.org/news/2010/05/27/15527/facebook-zuckerberg-argues-against-making-privacy/> (last accessed Apr. 1, 2021) (emphases added).

²⁰⁴ Mark Zuckerberg, *Our Commitment to the Facebook Community*, Facebook Newsroom (Nov. 29, 2011), available at <https://about.fb.com/news/2011/11/our-commitment-to-the-facebook-community/> (last accessed Apr. 1, 2021) (emphasis added).

²⁰⁵ *Id.* (emphases added).

1 g) Mark Zuckerberg's February 1, 2012 statement to prospective shareholders
 2 in connection with Facebook's IPO filing, indicating that "At Facebook, we build tools to help
 3 people connect with the people they want and **share what they want**[.] . . . We also believe that
 4 **giving people control over what they share is a fundamental principle**[.]"²⁰⁶

5 h) Facebook's September 30, 2012 statement, posted on its Newsroom,
 6 indicating that "We . . . recognize that **our users trust us to protect the information they share**
 7 on Facebook. **Maintaining that trust is a top priority** as we continue to grow."²⁰⁷

8 i) Mark Zuckerberg's June 8, 2013 statement, posted on Facebook's
 9 Newsroom, regarding Edward Snowden's allegations of government surveillance: "We will
 10 continue fighting aggressively to keep your information safe and secure."²⁰⁸

11 j) Mark Zuckerberg's March 13, 2014 statement on his own Facebook page
 12 responding to allegations that the National Security Agency posed as Facebook during a
 13 controversial surveillance program: "To keep the internet strong, we need to keep it secure. That's
 14 why at Facebook **we spend a lot of our energy making our services and the whole internet safer**
 15 **and more secure**. . . . Together, we can build a space that is greater and a more important part of
 16 the world than anything we have today, but is also safe and secure. **I'm committed to seeing this**
 17 **happen, and you can count on Facebook to do our part**."²⁰⁹

18 k) Facebook Product Manager Melissa Luu-Van's July 30, 2015 statement,
 19 posted on Facebook's Newsroom, indicating that: "We want everyone to have a safe experience on
 20

21 ²⁰⁶ Reuters Staff, *Zuckerberg's letter to investors*, Reuters (Feb. 1, 2012), available at
 22 [https://www.reuters.com/article/us-facebook-letter/zuckerbergs-letter-to-investors-idUSTRE8102](https://www.reuters.com/article/us-facebook-letter/zuckerbergs-letter-to-investors-idUSTRE8102MT20120201)
[MT20120201](https://www.reuters.com/article/us-facebook-letter/zuckerbergs-letter-to-investors-idUSTRE8102MT20120201) (last accessed Apr. 1, 2021) (emphases added).

23 ²⁰⁷ Facebook, *Relevant Ads That Protect Your Privacy*, Facebook Newsroom (Sept. 30,
 24 2012), available at <https://about.fb.com/news/2012/09/relevant-ads-that-protect-your-privacy/> (last
 accessed Apr. 1, 2021) (emphases added).

25 ²⁰⁸ Mark Zuckerberg, *Personal Response From Mark Zuckerberg About PRISM*, Facebook
 26 Newsroom (June 8, 2013), available at [https://about.fb.com/news/2013/06/personal-response-](https://about.fb.com/news/2013/06/personal-response-from-mark-zuckerberg-about-prism/)
[from-mark-zuckerberg-about-prism/](https://about.fb.com/news/2013/06/personal-response-from-mark-zuckerberg-about-prism/) (last accessed Apr. 1, 2021).

27 ²⁰⁹ Nicholas Carlson, *Zuckerberg: I Just Called Obama To Say How Mad I Am About The*
 28 *NSA*, Yahoo! News (Mar. 13, 2014), available at [https://www.yahoo.com/news/zuckerberg-obama-](https://www.yahoo.com/news/zuckerberg-obama-nsa-damaging-future-192935379.html)
[nsa-damaging-future-192935379.html](https://www.yahoo.com/news/zuckerberg-obama-nsa-damaging-future-192935379.html) (last accessed Apr. 1, 2021) (emphases added).

Facebook. That’s why we have dedicated teams and intelligent security systems working around the clock to help keep your account secure.”²¹⁰

l) Facebook’s statement in its 2016 10-K filing that while “some of our developers or other partners, such as those that help us measure the effectiveness of ads, may receive or store information provided by us or by our users through mobile or web applications integrated with Facebook[,]” Facebook only “provide[s] **limited information to such third parties** based on the scope of services provided to us.”²¹¹

m) Mark Zuckerberg’s March 2016 public statement in response to a statement issued by its subsidiary, WhatsApp, assuring that “Facebook stands with many technology companies to protect you and your information.”²¹²

n) Mark Zuckerberg’s March 12, 2017 public statement, posted on his Facebook page, that “[k]eeping the global community safe is an important part of our mission – and an important part of how we’ll measure our progress going forward” and reassurance that “[k]eeping our community safe does not require compromising privacy.”²¹³

o) Mark Zuckerberg’s March 21, 2018 statement following news outlets’ reporting on the Cambridge Analytica scandal that “[w]e have a responsibility to protect your data, and if we can’t then we don’t deserve to serve you.”²¹⁴

²¹⁰ Melissa Luu-Van, *Enhancing Security with a Quick Checkup*, Facebook Newsroom (July 30, 2015), available at <https://about.fb.com/news/2015/07/enhancing-security-with-a-quick-checkup/> (last accessed Apr. 1, 2021).

²¹¹ Form 10-K Filing for Facebook, Inc., Securities and Exchange Commission, available at <https://www.sec.gov/Archives/edgar/data/1326801/000132680117000007/fb-12312016x10k.htm> (last accessed Apr. 1, 2021) (emphasis added).

²¹² Anita Balakrishnan, Sara Salinas, and Matt Hunter, *Mark Zuckerberg has been talking about privacy for 15 years – here’s almost everything he’s said*, CNBC (Apr. 9, 2018), available at <https://www.cnn.com/2018/03/21/facebook-ceo-mark-zuckerbergs-statements-on-privacy-2003-2018.html> (last accessed Apr. 1, 2021).

²¹³ Mark Zuckerberg, *Building Global Community*, Facebook (Mar. 12, 2017), available at https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634?gid=339663931&mf_story_key=10103508221158471 (last accessed Apr. 1, 2021).

²¹⁴ *Facebook’s Zuckerberg speaks out over Cambridge Analytica ‘breach’*, BBC News (Mar. 22, 2018), available at <https://www.bbc.com/news/world-us-canada-43494337> (last accessed Apr. 1, 2021).

1 239. Facebook’s statements regarding its commitments to its users’ privacy and its
2 representations regarding its collection and sharing of their data were false, or, at a minimum,
3 omitted material facts that would be necessary to make these statements not misleading. These
4 representations left the false impression that Facebook allowed its users to choose specifically what
5 data Facebook could collect, to whom that data would be shared, and how it would be used.

6 240. Plaintiffs and Class members did not discover, nor could they have discovered
7 through reasonable diligence, that Facebook was deceiving them and violating the antitrust and
8 other laws until less than four years before this litigation was initially commenced. Facebook did
9 not tell Plaintiffs or other Class members that it was violating its 2011 Settlement with the FTC,
10 deceiving consumers and selling their data to extract revenue from third parties, or exploiting
11 consumers’ trust by surveilling them and using their data to identify competitors to “acquire, copy,
12 or kill.”

13 241. To the contrary, Mark Zuckerberg—Facebook’s founder, Chief Executive Officer,
14 and public face—repeatedly represented otherwise. Indeed, in announcing its largest-ever \$5
15 billion fine against Facebook following the Cambridge Analytica scandal, the FTC explained that
16 Facebook “encourages users to share information on its platform” by “promis[ing] users they can
17 control the privacy of their information,” but that Facebook “repeatedly used deceptive disclosures
18 and settings to undermine users’ privacy preferences[.]”

19 242. In addition, Facebook’s anticompetitive conduct was, by its very nature, inherently
20 self-concealing because it was performed outside the sight and knowledge of consumers. As a
21 result, Plaintiffs and Class members did not—and could not—discover Facebook’s scheme, even
22 with the exercise of reasonable diligence.

23 243. Plaintiffs and Class members attempted to exercise reasonable diligence in
24 maintaining the safety, security, and privacy of their data. That is why—based upon Facebook’s
25 avowed commitments to its users’ privacy—Plaintiffs and Class members used Facebook and its
26 various product offerings. Plaintiffs and Class members, however, did not discover, and could not
27 have reasonably discovered, their claims through the exercise of reasonable diligence until
28

consulting with counsel shortly before the filing of this action, and in any event, no earlier than March 2018.

D. Continuing Violations and Ascertainment of Damages

244. Since the start of the class period, Facebook has committed continuing violations of the antitrust laws, resulting in monetary injury to Plaintiffs and Class members. As described herein, Facebook has engaged in a pattern of independent misrepresentations to users, designed to acquire, maintain, and prolong Facebook’s monopoly position. Similarly, Facebook has weaponized its users’ data as a part of its serial acquisition strategy to “acquire, copy, or kill” its competitors.

245. Each of these injurious acts were separate and independent overt acts during the limitations period that were new and independent acts that inflicted new and accumulating injuries on consumers. Each of Facebook’s instances of deception as to its data privacy practices and commercial surveillance over time were acts new and independent from its past issues with data privacy and commercial surveillance. Facebook’s continued exposure of private information to app developers, advertisers, and other third parties leading up to 2018, as well as its anticompetitive acquisition practices, were additional, independent, and overt acts that harmed competition and inflicted new and accumulating economic injuries on consumers.

246. Moreover, Plaintiffs’ and Class members’ harms were not ascertainable—sufficient to give rise to the claims presented herein—more than four years prior to the date that this action was first commenced. Since the harm that Plaintiffs and Class members allege had not crystallized more than four years prior to the date that this action was initiated, the antitrust claims presented herein are timely.

VI. CLASS ACTION ALLEGATIONS

247. Plaintiffs re-allege and incorporate by reference herein all the allegations contained above.

248. Pursuant to Federal Rule of Civil Procedure 23(b)(3), Plaintiffs assert claims on behalf of **The Consumer Class**: All persons in the United States who maintained a Facebook profile at any point from 2007 up to the date of the filing of this action. Excluded from the Class

are Facebook, any entity in which Facebook has an interest, and any of Facebook's corporate parents, affiliates, subsidiaries, officers, directors, legal representatives, successors, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

249. This action has been brought and may properly be maintained as a class action as it satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of Rule 23(b)(3). Plaintiffs seek to represent an ascertainable Class, as determining inclusion in the Class can be done through Facebook's own records.

250. Although the precise number of Class members is unknown and can only be determined through appropriate discovery, the proposed Class numbers at least in the tens of millions and is therefore so numerous that joinder of all members would be impracticable.

251. Questions of law and fact common to the putative Class exist that predominate over questions affecting only individual members, including:

a) Whether Facebook's deception of consumers about its data privacy practices was anticompetitive;

b) Whether Facebook's acquisition conduct was anticompetitive;

c) Whether Facebook intentionally engaged in anticompetitive acts in order to obtain or maintain monopoly power;

d) Whether Facebook is a monopolist in the Social Network Market;

e) Whether Facebook is a monopolist in the Social Media Market;

f) Whether Facebook intentionally made material misrepresentations about its data privacy practices and the extent of its commercial surveillance;

g) Whether Facebook's foreclosure of competition in the Social Network Market caused by its anticompetitive conduct led to cognizable and quantifiable economic harms to consumers;

h) Whether Facebook's foreclosure of competition in the Social Media Market caused by its anticompetitive conduct led to cognizable and quantifiable economic harms to consumers;

i) Whether consumers would have had more options and competition amongst social networks and social media companies if Facebook would have revealed the full extent of its data privacy practices and commercial surveillance long ago;

j) Whether Facebook's anticompetitive conduct substantially harmed competition in the Social Network Market in the United States;

k) Whether Facebook's anticompetitive conduct substantially harmed competition in the Social Media Market in the United States; and

l) Whether Facebook's anticompetitive conduct should be enjoined or whether other appropriate equitable relief is just and proper, including ordering Facebook to divest assets or submit to more invasive third-party audits of its privacy practices and commercial surveillance.

252. Plaintiffs are members of the putative Consumer Class. The claims asserted by Plaintiffs in this action are typical of the claims of the members of the putative Consumer Class, as the claims arise from the same course of conduct by the Defendant and the relief sought is common.

253. Plaintiffs will fairly and adequately represent and protect the interests of the members of the putative Consumer Class, as their interests are coincident with, not antagonistic to, the other members of the Consumer Class.

254. Plaintiffs have retained counsel competent and experienced in both antitrust and class action litigation.

255. Certification of the Consumer Class is appropriate pursuant to Fed. R. C. P. 23(b)(3) because questions of law or fact common to the respective members of the Class predominate over questions of law or fact affecting only individual members. This predominance makes class litigation superior to any other method available for the fair and efficient adjudication of these claims including consistency of adjudications. Absent a class action, it would be unlikely that many members of the Consumer Class would be able to protect their own interests because the cost of litigation through individual lawsuits might exceed the expected recovery.

256. A class action is a superior method for the adjudication of the controversy in that it will permit a large number of claims to be resolved in a single forum simultaneously, efficiently, and without the unnecessary hardship that would result from the prosecution of numerous

individual actions and the duplication of discovery, effort, expense, and the burden of the courts that individual actions would create.

257. In the alternative, the Consumer Class should be certified because:

a) The prosecution of separate actions by the individual members of the proposed class would create a risk of inconsistent adjudications, which could establish incompatible standards of conduct for Facebook;

b) The prosecution of individual actions could result in adjudications, which as a practical matter, would be dispositive of the interests of non-party class members or which would substantially impair their ability to protect their interests; and

c) Facebook has acted or refused to act on grounds generally applicable to the proposed Consumer Class, thereby making appropriate final and injunctive relief with respect to the members of the proposed Consumer Class as a whole.

VII. INTERSTATE TRADE AND COMMERCE

258. Plaintiffs re-allege and incorporate by reference herein all the allegations contained above.

259. Facebook's anticompetitive conduct has taken place in, and negatively affected the continuous flow of interstate trade and commerce in the United States in that, *inter alia*:

a) Facebook has provided a social network and social media applications and has exchanged consumer information and attention with advertisers and consumers throughout the United States;

b) Facebook has used instrumentalities of interstate commerce to provide social network and social media services to consumers and advertisers throughout the United States;

c) In furtherance of the anticompetitive scheme alleged herein, Facebook has traveled between states and exchanged communications through interstate wire communications and via the United States mail; and

d) The anticompetitive scheme alleged herein has affected billions of dollars of commerce. Facebook has inflicted antitrust injury by artificially raising the cost to consumers of using its products, in terms of personal information and attention, by providing reduced user privacy

protections to consumers in exchange for their personal data, and by artificially reducing consumer choice and competition in the Social Network and Social Media Markets in the United States.

VIII. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF: MONOPOLIZATION OF SOCIAL NETWORK MARKET

Sherman Antitrust Act, § 2

(On behalf of the Consumer Class)

260. Plaintiffs re-allege and incorporate by reference herein all the allegations contained above.

261. Facebook has willfully acquired and maintained monopoly power in the relevant Social Network Market. There are no reasonably interchangeable products that would effectively constrain, or have effectively constrained, Facebook from imposing and profitably sustaining during the relevant period a significant artificial decrease in compensation to consumers for their user information and attention paid to advertisements. Facebook also has the power to impose and profitably sustain lower levels of data privacy protections and social network quality than would occur in a world where Facebook had not illegally monopolized the Social Network Market. Facebook has the power to control prices and exclude competition in the Social Network Market.

262. By multiple measures, Facebook has dominant market share in the Social Network Market. As discussed more fully below, Facebook's market share in the Social Network Market is higher than its share in the Social Media Market. And, more than 80% of the time that consumers in the United States spend using social media is spent on Facebook and Instagram.

263. High barriers to entry, high switching costs, and strong direct and indirect network effects make it unlikely, at any time in the foreseeable future, for a competitor to enter or take away substantial market share from Facebook in the Social Network Market in the United States to compete effectively with Facebook.

264. Facebook has willfully acquired and maintained monopoly power in the Social Network Market by means of predatory, exclusionary, and anticompetitive conduct. Such conduct includes, but is not limited to: (a) engaging in a scheme to gain market share at the expense of its rivals by inducing consumers to join Facebook through a pattern of deception regarding Facebook's

1 data privacy protections and its commercial surveillance; and (b) weaponizing the data it obtained
2 from consumers by means of deception to destroy competition through its strategy to “acquire,
3 copy, or kill” any and all of its competitors.

4 265. By eliminating competition and obtaining and maintaining monopoly power over
5 the Social Network Market as described above, Facebook was able to, and did, artificially decrease
6 compensation to consumers for their information and attention and provide lower value to
7 consumers than it would have provided in a competitive market.

8 266. Facebook’s destruction of competition caused antitrust injury to Plaintiffs and
9 Consumer Class members by decreasing compensation and lowering value for consumers, who
10 received lower compensation and lower value from Facebook than those consumers would have
11 received in the but-for world where Facebook competed on the merits. Plaintiffs and the Consumer
12 Class were injured and received substantially less compensation and lower value than they would
13 have absent Facebook’s unlawful and anticompetitive conduct.

14 267. During the relevant period, Plaintiffs and Consumer Class members gave Facebook
15 their personal data and attention in exchange for the use of its social network. As a result of
16 Facebook’s illegal conduct, Plaintiffs and other Consumer Class members received lower
17 compensation and value than they would have absent Facebook’s illegal conduct.

18 268. There are no legitimate pro-competitive or business justifications for the conduct
19 alleged herein, and even if there were, the anticompetitive effects would far outweigh any possible
20 pro-competitive effects.

21 269. Facebook’s acts and practices have continued to be anticompetitive in nature and
22 tendency and constitute an unfair method of competition, in violation of Section 2 of the Sherman
23 Act, 15 U.S.C. § 2.

24 270. Facebook’s conduct has had a substantial effect on interstate commerce.

25 271. Plaintiffs and Consumer Class members have been, and will continue to be, injured
26 in their property as a result of Facebook’s conduct.

27 272. Plaintiffs and Consumer Class members have suffered, and will continue to suffer,
28 injury of the type that the antitrust laws were intended to prevent, including but not limited to: (a)

1 lower compensation for their time and attention; (b) a reduction in consumer choice; and (c) being
 2 forced to accept a service of lesser quality because of reduced competition.

3 273. Plaintiffs and Consumer Class members seek an award of treble damages or, in the
 4 alternative, disgorgement of Facebook's ill-gotten gains. Plaintiffs also seek appropriate equitable
 5 relief to enjoin Facebook from continuing to engage in anticompetitive behavior to the detriment
 6 of consumers and to remedy the harms that Facebook's monopolization of the Social Network
 7 Market has caused, including: (a) divestment of assets that would continue to entrench its monopoly
 8 power; and (b) requiring Facebook to submit to independent monitoring of its user privacy
 9 practices, data surveillance, and acquisition conduct.

10 **SECOND CLAIM FOR RELIEF: ATTEMPTED MONOPOLIZATION OF SOCIAL**
 11 **NETWORK MARKET**

12 **Sherman Antitrust Act, § 2**

13 **(On behalf of the Consumer Class)**

14 274. Plaintiffs re-allege and incorporate by reference herein all the allegations contained
 15 above.

16 275. With respect to the Social Network Market, Facebook has engaged in predatory,
 17 exclusionary, and anticompetitive conduct, including but not limited to; (a) obtaining market share
 18 through a pattern of deceiving consumers; and (b) exploiting the data it obtained from consumers
 19 through deception to systematically destroy competition through its strategy to "copy, kill, or
 20 acquire" any and all of its competitors.

21 276. Facebook's conduct has had an anticompetitive effect in the Social Network Market.

22 277. Facebook's conduct has no legitimate business purpose or procompetitive effect,
 23 and even if there were, the anticompetitive effects would far outweigh any possible pro-competitive
 24 effects.

25 278. Facebook has engaged in the anticompetitive conduct described herein with the
 26 specific intent of monopolizing the Social Network Market.

27 279. Facebook has engaged in the anticompetitive conduct described herein with a
 28 dangerous probability of monopolizing the Social Network Market.

1 280. Facebook's conduct has had a substantial effect on interstate commerce.

2 281. Plaintiffs and Consumer Class members have been, and will continue to be, injured
3 in their property as a result of Facebook's conduct.

4 282. Plaintiffs and Consumer Class members have suffered, and will continue to suffer,
5 injury of the type that the antitrust laws were intended to prevent, including but not limited to: (a)
6 lower compensation for their time and attention; (b) a reduction in consumer choice; and (c) being
7 forced to accept a service of lesser quality because of reduced competition.

8 283. Plaintiffs and Consumer Class members seek an award of treble damages or, in the
9 alternative, disgorgement of Facebook's ill-gotten gains. Plaintiffs also seek appropriate equitable
10 relief to enjoin Facebook from continuing to engage in anticompetitive behavior to the detriment
11 of consumers and to remedy the harms that Facebook's attempted monopolization of the Social
12 Network Market has caused, including: (a) divestment of assets that would continue to entrench its
13 monopoly power; and (b) requiring Facebook to submit to independent monitoring of its user
14 privacy practices, data surveillance, and acquisition conduct.

15 **THIRD CLAIM FOR RELIEF: MONOPOLIZATION OF SOCIAL MEDIA MARKET**

16 **Sherman Antitrust Act, § 2**

17 **(On behalf of the Consumer Class)**

18 284. Plaintiffs re-allege and incorporate by reference herein all the allegations contained
19 above.

20 285. Facebook has willfully acquired and maintained monopoly power in the relevant
21 Social Media Market. There are no reasonably interchangeable products that would effectively
22 constrain, or have effectively constrained, Facebook from imposing and profitably sustaining
23 during the relevant period a significant artificial decrease in compensation to consumers for their
24 user information and attention paid to advertisements. Facebook also has the power to impose and
25 profitably sustain lower levels of data privacy protections and social media quality than would
26 occur in a world where Facebook had not illegally monopolized the Social Media Market.
27 Facebook has the power to control prices and exclude competition in the Social Media Market.
28

1 286. By multiple measures, Facebook has dominant market share in the Social Media
2 Market. As measured by advertising revenue that is generated by social media applications in the
3 Social Media Market, Facebook (including Instagram) has market share of at least 85% of the
4 Social Media Market. By its own measure, and as reflected in Facebook’s internal documents,
5 Facebook has estimated that it is “95% of all social media in the US[.]” And, more than 80% of
6 the time that consumers in the United States spend using social media is spent on Facebook and
7 Instagram.

8 287. High barriers to entry, high switching costs, and strong direct and indirect network
9 effects make it unlikely, at any time in the foreseeable future, for a competitor to enter or take away
10 substantial market share from Facebook in the Social Media Market in the United States to compete
11 effectively with Facebook.

12 288. Facebook has willfully acquired and maintained monopoly power in the Social
13 Media Market by means of predatory, exclusionary, and anticompetitive conduct. Such conduct
14 includes, but is not limited to: (a) engaging in a scheme to gain market share at the expense of its
15 rivals by inducing consumers to join Facebook through a pattern of deception regarding Facebook’s
16 data privacy protections and its commercial surveillance; and (b) weaponizing the data it obtained
17 from consumers by means of deception to destroy competition through its strategy to “acquire,
18 copy, or kill” any and all of its competitors.

19 289. By eliminating competition and obtaining and maintaining monopoly power over
20 the Social Media Market as described above, Facebook was able to, and did, artificially decrease
21 compensation to consumers for their information and attention and provide lower value to
22 consumers than it would have provided in a competitive market.

23 290. Facebook’s destruction of competition caused antitrust injury to Plaintiffs and
24 Consumer Class members by decreasing compensation and lowering value for consumers, who
25 received lower compensation and lower value from Facebook than those consumers would have
26 received in the but-for world where Facebook competed on the merits. Plaintiffs and Antitrust
27 Consumer Class members were injured and received substantially less compensation and lower
28 value than they would have absent Facebook’s unlawful and anticompetitive conduct.

1 291. During the relevant period, Plaintiffs and Consumer Class members gave Facebook
2 their personal data and attention in exchange for the use of its social media offerings. As a result
3 of Facebook's illegal conduct, Plaintiffs and other Consumer Class members received lower
4 compensation and value than they would have absent Facebook's illegal conduct.

5 292. There are no legitimate pro-competitive or business justifications for the conduct
6 alleged herein, and even if there were, the anticompetitive effects would far outweigh any possible
7 pro-competitive effects.

8 293. Facebook's acts and practices have continued to be anticompetitive in nature and
9 tendency and constitute an unfair method of competition, in violation of Section 2 of the Sherman
10 Act, 15 U.S.C. § 2.

11 294. Facebook's conduct has had a substantial effect on interstate commerce.

12 295. Plaintiffs and Consumer Class members have been, and will continue to be, injured
13 in their property as a result of Facebook's conduct.

14 296. Plaintiffs and Consumer Class members have suffered, and will continue to suffer,
15 injury of the type that the antitrust laws were intended to prevent, including but not limited to: (a)
16 lower compensation for their time and attention; (b) a reduction in consumer choice; and (c) being
17 forced to accept a service of lesser quality because of reduced competition.

18 297. Plaintiffs and Consumer Class members seek an award of treble damages or, in the
19 alternative, disgorgement of Facebook's ill-gotten gains. Plaintiffs also seek appropriate equitable
20 relief to enjoin Facebook from continuing to engage in anticompetitive behavior to the detriment
21 of consumers and to remedy the harms that Facebook's monopolization of the Social Media Market
22 has caused, including: (a) divestment of assets that would continue to entrench its monopoly power;
23 and (b) requiring Facebook to submit to independent monitoring of its user privacy practices, data
24 surveillance, and acquisition conduct.

**FOURTH CLAIM FOR RELIEF: ATTEMPTED MONOPOLIZATION OF SOCIAL
MEDIA MARKET**

Sherman Antitrust Act, § 2

(On behalf of the Consumer Class)

298. Plaintiffs re-allege and incorporate by reference herein all the allegations contained above.

299. With respect to the Social Media Market, Facebook has engaged in predatory, exclusionary, and anticompetitive conduct, including but not limited to; (a) obtaining market share through a pattern of deceiving consumers; and (b) exploiting the data it obtained from consumers through deception to systematically destroy competition through its strategy to “copy, kill, or acquire” any and all of its competitors.

300. Facebook’s conduct has had an anticompetitive effect in the Social Media Market.

301. Facebook’s conduct has no legitimate business purpose or procompetitive effect, and even if there were, the anticompetitive effects would far outweigh any possible pro-competitive effects.

302. Facebook has engaged in the anticompetitive conduct described herein with the specific intent of monopolizing the Social Media Market.

303. Facebook has engaged in the anticompetitive conduct described herein with a dangerous probability of monopolizing the Social Media Market.

304. Facebook’s conduct has had a substantial effect on interstate commerce.

305. Plaintiffs and Consumer Class members have been, and will continue to be, injured in their property as a result of Facebook’s conduct.

306. Plaintiffs and Consumer Class members have suffered, and will continue to suffer, injury of the type that the antitrust laws were intended to prevent, including but not limited to: (a) lower compensation for their time and attention; (b) a reduction in consumer choice; and (c) being forced to accept a service of lesser quality because of reduced competition.

307. Plaintiffs and Consumer Class members seek an award of treble damages or, in the alternative, disgorgement of Facebook’s ill-gotten gains. Plaintiffs also seek appropriate equitable

1 relief to enjoin Facebook from continuing to engage in anticompetitive behavior to the detriment
 2 of consumers and to remedy the harms that Facebook’s attempted monopolization of the Social
 3 Media Market has caused, including: (a) divestment of assets that would continue to entrench its
 4 monopoly power; and (b) requiring Facebook to submit to independent monitoring of its user
 5 privacy practices, data surveillance, and acquisition conduct.

6 **FIFTH CLAIM FOR RELIEF: UNJUST ENRICHMENT**

7 **California Common Law**

8 **(On behalf of the Consumer Class)**

9 308. Plaintiffs re-allege and incorporate by reference herein all the allegations contained
 10 above.

11 309. Facebook has been unjustly enriched through its misconduct as alleged herein.

12 310. Plaintiffs and Consumer Class members conferred direct benefits on Facebook in
 13 the forms of their personal data, time, and attention.

14 311. These benefits are quantifiable in measurable units. Facebook sells access to its
 15 users’ data, time, and attention to third parties—including advertisers and app developers—for
 16 discrete money amounts. In 2019, for example, Facebook collected \$70.7 billion in revenue, almost
 17 entirely from allowing companies to serve ads to its users. That year, Facebook itself reported that
 18 its ARPU was over \$41.00 per user in the United States and Canada.

19 312. Facebook appreciated and had knowledge of the fact that Plaintiffs and Consumer
 20 Class members conferred these benefits on it. For example, after Facebook’s involvement in the
 21 Cambridge Analytica scandal came to light in March 2018, Facebook founder Mark Zuckerberg
 22 explicitly recognized that Plaintiffs and Consumer Class members conferred on Facebook the
 23 benefit of their data, stating: “We have a responsibility to protect your data, and if we can’t then
 24 we don’t deserve to serve you.” That Facebook internally tracks the time its users spend on
 25 Facebook (and its family of products) and compares these figures to the time they spend on other
 26 competing services further makes clear that Facebook recognizes Plaintiffs and Consumer Class
 27 members have conferred on it the benefits of their time and attention.
 28

1 313. Facebook acquired these benefits from Plaintiffs and Consumer Class members
 2 through the misrepresentations and deception it and its executives publicly promulgated. Facebook
 3 induced Plaintiffs and Consumer Class members to join Facebook based on the promise of stringent
 4 privacy protections. All the while, Facebook concealed the scope of the data it harvested from
 5 Plaintiffs and Consumer Class members and brokered to third parties. Nor did Facebook reveal the
 6 manner in which it weaponized Plaintiffs' and Consumer Class members' data to "copy, kill, or
 7 acquire" Facebook's rivals.

8 314. As a result of Facebook's receipt of the direct benefits of Plaintiffs' and Consumer
 9 Class members' data, time, and attention, Facebook was able to destroy competition, enriching
 10 itself at the expense of Plaintiffs and Consumer Class members. Although Plaintiffs and Consumer
 11 Class member conferred on Facebook the direct benefits of their data, time, and attention, Plaintiffs
 12 and Consumer Class members have been, as a result of Facebook's misconduct: (a) deprived of a
 13 marketplace that adequately compensates them for their data, time, and attention with benefits of
 14 reciprocal value; (b) forced to accept Facebook's services, which are of inferior quality, with no
 15 meaningful alternative.

16 315. Facebook has unjustly reaped monstrous financial gain as a result of the misconduct
 17 alleged herein. In 2019, for example, Facebook collected \$70.7 billion in revenue, almost entirely
 18 from allowing companies to serve ads to its users. It would be unfair, unscrupulous, unjust, and
 19 inequitable to allow Facebook to retain the value it derived from the direct benefits that Plaintiffs
 20 and Consumer Class members conferred upon it.

21 316. To the extent that it is required—and solely in the alternative—Plaintiffs and
 22 Consumer Class members have no other adequate remedy at law available.

23 317. Plaintiffs and Consumer Class members in all of the 50 States and the District of
 24 Columbia accordingly seek disgorgement of all of Facebook's profits resulting from the wanton
 25 misconduct alleged herein.

26 **IX. PRAYER FOR RELIEF**

27 318. WHEREFORE, Plaintiffs Maximilian Klein, Sarah Grabert, and Rachel Banks
 28 Kupcho, on behalf of themselves and the Consumer Class, seek the following relief:

1 **a)** An order certifying this action as a class action under Fed. R. Civ. P. 23,
2 defining the Consumer Class as requested herein, finding that Plaintiffs are proper representatives
3 of the Consumer Class requested herein, and appointing Plaintiffs' counsel as Consumer Class
4 Counsel.

5 **b)** Injunctive and other equitable relief as is necessary to protect the interests of
6 the Consumer Class, including: (i) an order prohibiting Facebook from continuing to engage in the
7 wrongful acts described herein; and (ii) requiring Facebook to engage third-party auditors to
8 conduct audits and evaluations of Facebook's data privacy practices, commercial surveillance, and
9 acquisition conduct, and ordering them to promptly correct any problems or issues detected by
10 these auditors.

11 **c)** Treble damages or, alternatively, restitution and/or disgorgement of all
12 amounts wrongfully charged to and received from Plaintiffs and Consumer Class members.

13 **d)** Attorneys' fees, statutory costs and other costs of suit herein incurred, for
14 both pre-judgment and post-judgment interest on any amounts awarded, for corrective advertising
15 to ameliorate consumers' mistaken impressions created by Facebook's anticompetitive conduct.

16 **e)** Declaratory relief, including but not limited to a declaration and judgment
17 that Facebook's conduct as alleged herein violates the laws alleged herein.

18 **f)** Such other relief as the Court may deem just and proper, such as divestiture
19 of assets that entrench Facebook's monopoly power.

20 **X. DEMAND FOR JURY TRIAL**

21 Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiffs hereby demand trial
22 by jury in this action of all issues so triable.
23
24
25
26
27
28

DATED: April 22, 2021

Respectfully submitted,

By /s/ Shana E. Scarlett

By /s/ Stephen A. Swedlow

HAGENS BERMAN SOBOL SHAPIRO LLP

QUINN EMANUEL URQUHART & SULLIVAN, LLP

Shana E. Scarlett (Bar No. 217895)

Stephen A. Swedlow (admitted *pro hac vice*)

shanas@hbsslaw.com

stephenswedlow@quinnemanuel.com

715 Hearst Avenue, Suite 202

Michelle Schmit (admitted *pro hac vice*)

Berkeley, CA 94710

michelleschmit@quinnemanuel.com

(510) 725-3000

191 N. Wacker Drive, Suite 2700

Chicago, IL 60606-1881

(312) 705-7400

Steve W. Berman (admitted *pro hac vice*)

steve@hbsslaw.com

Kevin Y. Teruya (Bar No. 235916)

kevinteruya@quinnemanuel.com

1301 Second Avenue, Suite 2000

Adam B. Wolfson (Bar No. 262125)

Seattle, WA 98101

adamwolfson@quinnemanuel.com

(206) 623-7292

Brantley I. Pepperman (Bar No. 322057)

brantleypepperman@quinnemanuel.com

LOCKRIDGE GRINDAL NAUEN P.L.L.P.

W. Joseph Bruckner (admitted *pro hac vice*)

865 South Figueroa Street, 10th Floor

wjbruckner@locklaw.com

Los Angeles, CA 90017-2543

(213) 443-3000

Robert K. Shelquist (admitted *pro hac vice*)

rkshelquist@locklaw.com

Manisha M. Sheth (admitted *pro hac vice*)

Brian D. Clark (admitted *pro hac vice*)

bdclark@locklaw.com

manishasheth@quinnemanuel.com

Rebecca A. Peterson (Bar No. 241858)

51 Madison Avenue, 22nd Floor

rapeterson@locklaw.com

New York, New York 10010

(212) 849-7000

Arielle S. Wagner (admitted *pro hac vice*)

aswagner@locklaw.com

KELLER LENKNER LLC

Warren Postman (Bar No. 330869)

Stephanie A. Chen (admitted *pro hac vice*)

sachen@locklaw.com

wdp@kellerlenkner.com

Jason Ethridge (admitted *pro hac vice*)

100 Washington Avenue South, Suite 2200

jason.ethridge@kellerlenkner.com

Minneapolis, MN 55401

1300 I Street, N.W., Suite 400E

Washington, DC 20005

(202) 918-1123

(612) 339-6900

Ashley Keller (admitted *pro hac vice*)

ack@kellerlenkner.com

Ben Whiting (admitted *pro hac vice*)

ben.whiting@kellerlenkner.com

Jason A. Zweig (admitted *pro hac vice*)

jaz@kellerlenkner.com

150 N. Riverside Plaza, Suite 4270

Chicago, IL 60606

(312) 741-5220

Interim Counsel for the Consumer Class

This document is being filed through the Electronic Case Filing (ECF) system by attorney Stephen A. Swedlow. By his signature, Mr. Swedlow attests that he has obtained concurrence in the filing of this document from each of the attorneys identified on the caption page and in the above signature block.

By /s/ Stephen A. Swedlow
Stephen A. Swedlow

I hereby certify that on this 22nd day of April 2021, I electronically transmitted the foregoing document to the Clerk's Office using the CM/ECF System, causing the document to be electronically served on all attorneys of record.

By /s/ Stephen A. Swedlow
Stephen A. Swedlow

ATTACHMENT B

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FILED UNDER SEAL

BATHAEE DUNNE LLP

Yavar Bathaee (CA 282388)
yavar@bathaeedunne.com
Edward M. Grauman (*pro hac vice*)
egrauman@bathaeedunne.com
Andrew C. Wolinsky
awolinsky@bathaeedunne.com
445 Park Avenue, 9th Floor
New York, NY 10022
Tel.: (332) 322-8835

Brian J. Dunne (CA 275689)
bdunne@bathaeedunne.com
633 West Fifth Street, 26th Floor
Los Angeles, CA 90071
Tel.: (213) 462-2772

*Interim Co-Lead Counsel for the
Advertiser Class*

SCOTT + SCOTT ATTORNEYS AT LAW LLP

Kristen M. Anderson (CA 246108)
kanderson@scott-scott.com
230 Park Avenue, 17th Floor
New York, NY 10169
Tel.: (212) 223-6444

Christopher M. Burke (CA 214799)
cburke@scott-scott.com
David H. Goldberger (CA 225869)
dgoldberger@scott-scott.com
Kate Lv (CA 302704)
klv@scott-scott.com
600 W. Broadway, Suite 3300
San Diego, CA 92101
Tel.: (619) 233-4565

Patrick J. McGahan (*pro hac vice*)
pmcgahan@scott-scott.com
Michael P. Srodoski (*pro hac vice*)
msrodoski@scott-scott.com
156 South Main Street, P.O. Box 192
Colchester, CT 06415
Tel.: (860) 537-5537

(Additional counsel on signature page)

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MAXIMILIAN KLEIN, et al., on behalf of themselves
and all others similarly situated,

Plaintiffs,

v.

META PLATFORMS, INC.,

Defendant.

Case No. 20-cv-08570-JD

The Hon. James Donato

**FIRST AMENDED CONSOLIDATED
ADVERTISER CLASS ACTION
COMPLAINT**

DEMAND FOR JURY TRIAL

CLASS ACTION

FILED UNDER SEAL**TABLE OF CONTENTS**

| | | |
|----|--|----|
| 1 | INTRODUCTION | 1 |
| 2 | PARTIES | 5 |
| 3 | I. PLAINTIFFS | 5 |
| 4 | II. DEFENDANT | 6 |
| 5 | JURISDICTION AND VENUE | 8 |
| 6 | INTRADISTRICT ASSIGNMENT | 9 |
| 7 | FACTS | 9 |
| 8 | I. FACEBOOK EMERGES AS THE DOMINANT SOCIAL NETWORK | 9 |
| 9 | A. The Last Social Network Standing | 9 |
| 10 | B. A New Market of Its Own Creation | 11 |
| 11 | C. The Data Targeting Barrier to Entry | 13 |
| 12 | D. Google's Failed Entry into the Social Advertising Market | 16 |
| 13 | II. A THREAT TO FACEBOOK'S MONOPOLY: THE RISE OF SMARTPHONES AND | |
| 14 | MOBILE APPS | 19 |
| 15 | A. The Mobile App Revolution | 19 |
| 16 | B. Facebook Recognizes the Looming Threat Presented by Mobile Applications | 22 |
| 17 | C. The Facebook Platform | 23 |
| 18 | D. The Profitable Open Graph Platform and Mobile Install Business | 26 |
| 19 | III. FACEBOOK WEAPONIZES ITS PLATFORM TO DESTROY COMPETITION | 28 |
| 20 | A. Facebook Makes Plans to Remove Vital Platform Functionality and Refuses to Sell | |
| 21 | Social Data to Competing Application Developers | 28 |
| 22 | B. Facebook's Social Data Heist | 31 |
| 23 | C. Facebook Targets Its Competitors for Reciprocity or Denial of API Access | 35 |
| 24 | D. Facebook Decides to Add the Events API to Its Reciprocity Scheme | 39 |
| 25 | E. The Decision to Remove Developer Access to the Friends, News Feed, Events, and | |
| 26 | Other Crucial APIs Lacked Any Legitimate Justification | 41 |
| 27 | F. Facebook Prepares to Announce Removal of the APIs | 45 |
| 28 | G. The Announcement at F8 | 49 |
| | IV. THE SURVEILLANCE AND ACQUISITION OF COMPETITIVE THREATS | 50 |
| | A. Facebook Relies on Onavo's Surveillance of Facebook's Competitors, and Acquires | |
| | and Uses Onavo's Assets | 51 |
| | B. Facebook Identifies Instagram as a Threat and Acquires the Company | 55 |

FILED UNDER SEAL

| | | |
|----|----------------------------------|----|
| C. | Facebook Acquires WhatsApp | 63 |
|----|----------------------------------|----|

The image shows a document that has been almost entirely redacted with thick black horizontal bars. On the left side, there are several small black rectangular markers, some of which are followed by a small yellow rectangular block. These markers appear to be part of a list or index, but the text they point to is obscured. The yellow blocks are located at the beginning of several lines of text, possibly indicating a specific section or a key point. The overall layout suggests a structured document, such as a report or a list of items, where the content has been withheld for security or privacy reasons.

FILED UNDER SEAL

| | | |
|-----|--|-----|
| IX. | THE THREAT BEYOND FACEBOOK’S WALLED GARDEN | 138 |
| A. | Facebook Audience Network | 138 |
| B. | Facebook Acquires Atlas..... | 140 |
| C. | Facebook Positions Itself Against Google by Combining Atlas, Audience Network, and Other Technology | 144 |
| D. | Shadow Profiles and Identifying Users Outside of Facebook’s Apps..... | 146 |
| X. | FACEBOOK AND GOOGLE AGREE NOT TO COMPETE AND TO FORTIFY THE FACEBOOK-DOMINATED SOCIAL ADVERTISING MARKET | 147 |
| A. | Google’s Dominance Over Ad Exchanges and Ad Servers and the Looming Facebook Threat..... | 147 |
| B. | Google’s AI Dominance | 149 |
| C. | The Rise of Header Bidding and Facebook’s Threat to Compete with Google | 151 |
| D. | Google Agrees to Help Facebook Identify Facebook’s Own Users Outside of Its Walled Garden, and Facebook Backs Off of Programmatic and Exchange-Trade Advertising | 153 |

FILED UNDER SEAL

| | | |
|-------|--|-----|
| XII. | THE RELEVANT MARKET | 181 |
| A. | The Social Advertising Market..... | 181 |
| B. | Barriers to Entry | 188 |
| C. | Relevant Geographic Market..... | 190 |
| XIII. | HARM TO COMPETITION AND ANTITRUST INJURY | 191 |
| | CLASS ACTION ALLEGATIONS | 195 |
| | CLAIMS FOR RELIEF | 201 |
| | PRAYER FOR RELIEF | 204 |
| | JURY DEMAND..... | 205 |

FILED UNDER SEAL**INTRODUCTION**

1
2 1. This Complaint is brought on behalf of people and companies—including each of the
3 named Plaintiffs—who bought advertising from Defendant Meta Platforms, Inc.¹ (“Facebook”) at
4 anticompetitively inflated prices. Over the course of the past decade, Facebook devised, executed, and
5 reaped the benefits of a scheme to unlawfully monopolize the market for social advertising. As a direct
6 result, Facebook was able to (and in fact, did) charge supracompetitive prices for social advertisements
7 to thousands of people and businesses, including Plaintiffs Affilious, Inc., Jessyca Frederick, Mark
8 Young, Joshua Jeon, 406 Property Services, PLLC, Mark Berney, and Katherine Looper.

9 2. Facebook acquired the power to raise prices through the anticompetitive scheme described
10 below and did so year after year with no competitive check.

11 * * *

12 3. By the end of 2010, Facebook had emerged the victor among social networks and had
13 begun monetizing its product through targeted advertising. Facebook had obtained a monopoly in a form
14 of online advertising that was distinct from others—social advertising. This form of advertising relied on
15 a particular form of data, called social data, to power machine learning and AI models used for advertising
16 and content targeting.

17 4. Facebook had acquired a critical mass of social data and targeting infrastructure, giving
18 rise to a Data Targeting Barrier to Entry (“DTBE”)—a network-driven barrier to entry that protected
19 Facebook’s monopoly share of the Social Advertising Market.

20 5. Facebook’s dominance was threatened in 2012, and to fend off this threat Facebook’s CEO
21 Mark Zuckerberg and his senior lieutenants planned and executed a scheme between 2012 and 2015 that
22 leveraged Facebook’s developer Platform to extract social data and advertising revenue from third-party
23 apps, some of which posed a competitive threat to Facebook. During this period, Facebook overtly
24 destroyed its actual and potential competition, and acquired two then-nascent threats to its business,
25 Instagram and WhatsApp.

26
27 ¹ Originally-named Defendant Facebook, Inc. changed its name to Meta Platforms, Inc., during
28 the pendency of this case.

FILED UNDER SEAL

1 6. By April 2015, Facebook had expelled third-party apps from its Platform, including by
2 purporting to deprecate core functionality such as traversing a user's Facebook friends, news feed, or
3 Events functionality. Before this move, Facebook had been able to harvest social data from apps built on
4 its Platform. Afterwards, however, Facebook faced a social data vacuum. Facebook entered into a series
5 of data sharing and whitelist agreements to obtain vital data and advertising revenue, [REDACTED]
6 [REDACTED]

7 7. Yet Facebook was still in need of what it [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]

12 8. To obtain data from these companies, from 2016 to 2018 Facebook entered targeted sub-
13 verticals, threatening ruinous competition and then [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27
28

FILED UNDER SEAL

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]

15 15. As the 2010s wore on, technological developments in header bidding and Google's
16 acquisition and deployment of powerful machine learning tools across its growing data collection
17 ecosystem threatened to erode Facebook's identity-based targeting advantage—and perhaps even
18 superset the Social Advertising Market. Facebook responded by acquiring and expanding powerful cross-
19 site and cross-device tracking tools, deploying its own machine learning tools outside its walled garden,
20 and laying the groundwork to enter programmatic advertising and other Google-dominated online ad
21 markets. By 2018, the two online advertising titans—each with its own long-running sphere of
22 dominance—were headed for a direct clash.

23 16. Except that instead of competing, Facebook and Google actually cut an anticompetitive
24 deal. Codenamed "Jedi Blue," this September 2018 agreement between Facebook and Google divided
25 markets between the two companies and not only reinforced but bolstered Facebook's dominant position
26 in the Social Advertising Market.
27
28

FILED UNDER SEAL

1 17. Pursuant to the Jedi Blue agreement, Facebook dropped its support for header bidding,
2 effectively ceding the programmatic and exchange-based ad markets to Google. At the same time, Google
3 agreed to provide Facebook powerful tools to identify, target, and monetize Facebook’s own users on the
4 web and across third-party mobile applications, then give Facebook priority over 90% of advertisements
5 to these users and twice the amount of time to bid on advertising to them.

6 18. The net effect was that Facebook remained the dominant—and only—source of granularly
7 targeted advertising to its social-networking user base. In exchange, Facebook backed away from
8 Google’s advertising exchange business, including by forgoing the adoption of “header bidding.”

9 19. As a result of the conduct set forth above, Facebook became and remained for nearly a
10 decade the dominant (and in many respects, sole) source for highly valuable advertising that could
11 precisely target networks of users in a social network. Facebook has used this market power to repeatedly
12 raise advertising prices every year since it began its scheme.

13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]

20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]

FILED UNDER SEAL

22. Over the course of nearly a decade, Facebook has faced no meaningful competitive check on social advertising prices—and it has extracted supracompetitive revenues from advertisers like Plaintiffs throughout this period.

23. Plaintiffs are advertisers on Facebook’s advertising platform that were injured by paying supracompetitive prices for social advertising. The prices they paid would have been lower if Facebook had not unlawfully monopolized the Social Advertising Market and taken unlawful acts (including an express anticompetitive agreement with Google) to maintain that monopoly, as those prices would have been subject to competitive forces that would otherwise exist as a check on Facebook’s market power and monopoly.

PARTIES**I. PLAINTIFFS**

24. Plaintiff Affilious, Inc. (“Affilious”) is a California corporation with its principal place of business in La Quinta, California. Affilious is an internet publisher firm that operates several websites, including WineClubReviews.net. In late 2016 and in August 2017, Affilious purchased advertising on Facebook’s self-service advertising platform to promote WineClubReviews.net. Until no earlier than November 6, 2019, Affilious did not know, and could not reasonably have known, the truth about Facebook’s anticompetitive conduct, including its purpose and intent to engage in anticompetitive conduct, nor could it have known that it had been injured by paying supracompetitive prices for advertising.

25. Plaintiff Jessyca Frederick is a citizen of the State of California. Frederick was the sole proprietor of ClubsAndGifts.com, a promotional website, and a founder and CEO of Affilious. At various times from April 4, 2009, through August 2017, Frederick purchased advertising on Facebook’s self-service advertising platform to promote her businesses.

26. Plaintiff Mark Young is a citizen of the State of New York. Young is the sole proprietor of Dinkum Hair, a hair salon located in Buchanan, New York. Young d/b/a Dinkum Hair purchased advertising on Facebook’s self-service advertising platform to promote the business between June 2017 and April 2019.

FILED UNDER SEAL

27. Plaintiff Joshua Jeon is a citizen of the State of Texas. He is a pastor at Dwell Church in Austin, Texas. In April 2016, Jeon purchased advertising on Facebook’s self-service advertising platform to promote Dwell Church. Jeon did not receive reimbursement from Dwell Church for the purchase.

28. Plaintiff 406 Property Services, PLLC (“406 Property Services”) is a Montana professional limited liability company with its principal place of business in Whitefish, Montana. 406 Property Services is a real estate property services company. From approximately June 8, 2017, until approximately October 20, 2017, 406 Property Services purchased advertising on Facebook’s self-service advertising platform to promote its business.

29. Plaintiff Mark Berney is a citizen of the State of Montana. From in or about 2016 into December 2018, Berney purchased advertising on Facebook’s self-service advertising platform to promote his personal musical work.

30. Plaintiff Katherine Looper is a citizen of the State of California. From in or about 2013 through March 2020, Looper purchased advertising on Facebook’s self-service advertising platform to promote free musical concerts at the Cadillac Hotel, a residential hotel for low-income persons in San Francisco operated by Looper’s nonprofit organization, Reality House West.

31. Plaintiffs all paid prices for advertising that were higher than they would have been absent Facebook’s anticompetitive conduct and unlawfully acquired and/or maintained monopoly. Facebook caused Plaintiffs to pay supracompetitive prices for advertising as a result of the market power it obtained and/or maintained as a result of the anticompetitive scheme described in this Complaint.

II. DEFENDANT

32. Defendant Meta Platforms, Inc., is a publicly traded company, incorporated in Delaware. Meta Platforms, Inc. was formerly known as Facebook, Inc., and changed its name to Meta Platforms, Inc. on October 28, 2021. Facebook’s principal place of business and headquarters is located at 1601 Willow Road in Menlo Park, California.

33. Founded in 2004 by Mark Zuckerberg, Facebook is a social media company that provides online services to billions of users around the world. In exchange for providing services, Facebook

FILED UNDER SEAL

collects user data, which it uses to create and sell targeted advertising services. Facebook's principal revenue is from targeted social media advertising that it provides to advertisers as a data broker.

34. Facebook also operates as a platform for third-party applications and hardware, and owns and operates several business divisions:

- Facebook. Facebook's core application, which bears the company's name, is, according to Facebook's filing with shareholders, designed to enable "people to connect, share, discover, and communicate with each other on mobile devices and personal computers." The Facebook core product contains a "News Feed" that displays an algorithmically ranked series of stories and advertisements individualized for each person.
- Instagram. Instagram is a photo-sharing application that allows users to share photos, videos, and messages on mobile devices. Instagram was acquired in April 2012, and at present, Facebook operates Instagram as a separate application from its core Facebook product.
- Messenger. Facebook's Messenger application is a multimedia messaging application, allowing messages that include photos and videos to be sent from person to person across platforms and devices.
- WhatsApp. WhatsApp is a secure messaging application used by individuals and businesses. WhatsApp was acquired by Facebook in 2014 for \$21.8 billion, and at the time had approximately 450 million users worldwide.
- Oculus. Oculus is Facebook's virtual reality hardware line of business, which Facebook acquired in March 2014 for approximately \$2 billion.

35. Facebook's revenue as of year-end 2019 was \$70.70 billion (up 27% from the previous year), with net income from operations of \$23.99 billion. Almost all of this revenue came from advertising, particularly mobile advertising. As of year-end 2019, Facebook maintained \$54.86 billion in cash and cash-equivalent securities. Facebook employed 44,942 people around the world at the end of 2019 (up 26% from the previous year). Facebook's revenue as of year-end 2020 was \$85.97 billion (a 22% increase from the previous year), with net income from operations of \$32.67 billion. Again, almost

FILED UNDER SEAL

all of that revenue came from mobile advertising. As of year-end 2020, Facebook maintained \$61.95 billion in cash and cash-equivalent securities. Facebook employed 58,604 people around the world at the end of 2020 (up 30% from the previous year). In 2021, Facebook / Meta earned \$117.93 billion in revenue, of which \$114.93 billion came from advertising. The company's 2021 total income from operations was \$46.753 billion. Disregarding Facebook / Meta's Reality Labs division (which operated at a substantial loss), Facebook / Meta's total income from operations in 2021 was \$56.95 billion. Facebook / Meta's net income from operations (including Reality Labs) in 2021 was \$39.37 billion

36. For the 2019 fiscal year, Facebook reported to investors that on average it had 1.66 billion daily active users of Facebook and Messenger ("DAUs") (up 9% from the previous year) and 2.50 billion monthly active users ("MAUs") (up 8% from the previous year). Facebook also reported that on average it had 2.26 billion daily active people ("DAP") who used any Facebook product (up 11% from the previous year) and 2.89 billion monthly active people ("MAP") (up 9% from the previous year). For the 2020 fiscal year, Facebook reported to investors that on average it had 1.84 billion DAUs (up 11% from the previous year) and 2.80 billion MAUs (up 12% from the previous year). Facebook also reported that on average it had 2.60 billion DAP who used any Facebook product (up 15% from the previous year). For the 2021 fiscal year, Facebook / Meta reported to investors that on average it had 1.91 billion DAUs, 2.89 billion MAUs, 2.78 billion DAP, and 3.53 billion MAP, across its family of products—an increase from 2020 in all four categories.

JURISDICTION AND VENUE

37. This action arises under Sections 1 and 2 of the Sherman Antitrust Act (15 U.S.C. §§ 1, 2) and Sections 4 and 16 of the Clayton Act (15 U.S.C. §§ 15, 26). The action seeks to recover treble damages, interest, costs of suit, equitable relief, and reasonable attorneys' fees for damages to Plaintiffs and members of the Classes resulting from Defendant's restraints of trade and monopolization of the Social Advertising Market described herein.

38. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 (federal question), 1332 (class action diversity jurisdiction), and 1337(a) (antitrust); and under 15 U.S.C. § 15 (antitrust).

FILED UNDER SEAL

39. Venue is appropriate in this district under 15 U.S.C. § 15(a) (Clayton Act), 15 U.S.C. § 22 (nationwide venue for antitrust matters), and 28 U.S.C. § 1391(b) (general venue provision). Facebook transacts business within this district, and it transacts its affairs and carries out interstate trade and commerce, in substantial part, in this district.

40. The Court has personal jurisdiction over Facebook as it is subject to general jurisdiction in the State of California, where it maintains its headquarters and its principal place of business. The scheme, conspiracy, and monopolization alleged in this Complaint was targeted at individuals throughout the United States, causing injury to persons in the United States, including in this district.

INTRADISTRICT ASSIGNMENT

41. This action has been assigned to the Hon. James Donato of the San Francisco Division of this judicial district.

FACTS**I. FACEBOOK EMERGES AS THE DOMINANT SOCIAL NETWORK****A. The Last Social Network Standing**

42. Facebook's meteoric rise since its founding in 2004 is well documented. The company—started in the dorm room of its CEO Mark Zuckerberg as “the facebook”—rose to prominence in the face of fierce competition from several social networks. Initially an exclusive service for elite universities throughout the United States, Facebook eventually expanded its network to encompass a general audience of users throughout the United States and worldwide.

43. Between 2004 and 2010, Facebook vanquished a number of rivals, emerging as the dominant social network in the United States.

44. Facebook's first chief competitor was MySpace. Founded in 2003 (a year before Facebook), MySpace targeted the same audience, provided largely the same services, and rapidly attracted an enormous number of users. By 2005, MySpace had 25 million active users, and was acquired by NewsCorp for \$580 million. In 2006, MySpace registered 100 million users, passing Google as the most visited website in the United States.

FILED UNDER SEAL

1 45. However, the next three years featured a steady downward spiral for MySpace—and
2 countervailing growth by Facebook. In 2008, Facebook passed MySpace in worldwide active users and
3 continued to grow, reaching 307 million active users across the globe by April 2009. In May 2009,
4 Facebook passed MySpace in United States, 70.28 million to 70.26 million monthly active users.

5 46. MySpace never came close to Facebook again. By 2010, MySpace had mostly exited the
6 market, leaving the business of social media for good. MySpace’s CEO capitulated in November of 2010:
7 “MySpace is not a social network anymore. It is now a social entertainment destination.” In September
8 2010, MySpace reported that it had lost \$126 million, and in June 2011, NewsCorp sold the company for
9 \$35 million—\$545 million less than it had paid just six years earlier. By then, its user base had dwindled
10 to just 3 million monthly visitors.

11 47. During the same time period, several other social networks also met their demise,
12 including Google’s Orkut, AOL’s Bebo, and Friendster, which failed to scale rapidly enough to compete
13 with MySpace and Facebook.

14 48. By 2009 and through 2010, Facebook emerged as the only peer-to-peer social media
15 network to exist at scale, and no other network or company rivaled Facebook’s massive user base. On
16 March 2, 2010, *Adweek* reported that Facebook had booked revenues of up to \$700 million in 2009 and
17 was on track for \$1.1 billion in 2010—almost all from advertising to its newly won users. Facebook had
18 been roughly doubling its revenues every year up until that point—\$150 million in 2007, \$280-300
19 million in 2008, and \$700 million in 2009.

FILED UNDER SEAL

49. *Time* magazine heralded Zuckerberg as its 2010 Person of the Year.



50. *Time*'s cover story set out the stakes—the scope of the newly assembled social network was unprecedented and staggering:

What just happened? In less than seven years, Zuckerberg wired together a twelfth of humanity into a single network, thereby creating a social entity almost twice as large as the U.S. If Facebook were a country it would be the third largest, behind only China and India. It started out as a lark, a diversion, but it has turned into something real, something that has changed the way human beings relate to one another on a species-wide scale. We are now running our social lives through a for-profit network that, on paper at least, has made Zuckerberg a billionaire six times over.

51. By 2010, Facebook was unrivaled and dominant in a way no company since Microsoft had been in post-personal-computer history. And it had done so by riding the currents of powerful network effects.

B. A New Market of Its Own Creation

52. By the beginning of the millennium's second decade, Facebook was the indisputable king of an entirely new market—a market built not on hardware or operating system dominance, but one built on a network of people, with its power and value directly derived from their engagement with that

FILED UNDER SEAL

1 network. The more data users fed into Facebook by communicating and interacting with each other,
2 posting their pictures, and publishing their content, the more valuable the Facebook network became to
3 third parties, who could advertise to Facebook's users by targeting them using the very information they
4 provided to Facebook's network.

5 53. Data about what information users shared on their personal pages; the photos and profiles
6 they viewed; their connections to others; what they shared with others; and even what they put in
7 messages to other users all allowed targeted advertising on a scale that had never before existed. Unlike
8 search advertising, Facebook's advertising platform allowed advertisers to target Facebook's user base
9 by their attributes and behavior, not by a query entered into a search box. More importantly, unlike in
10 search, user identity was not only discoverable, it was willingly provided by users—as was the identity
11 of those users' closest friends and family members. These identities could be tracked and targeted
12 throughout the Internet.

13 54. This social data created by Facebook's network of engaged users could be monetized in a
14 number of ways. The data could be resold for targeted advertising and machine learning; Facebook's
15 machine learning algorithms mined patterns in the data for advertisers, which allowed advertisers to reach
16 precisely the right audience to convert into sales, user sign-ups, or the generation of sales leads. The data
17 also could be sold by commercializing access—for example, by providing application developers, content
18 generators, and advertisers with direct access to the information embedded in Facebook's network, such
19 as the interconnection between users, user attributes, and user behavior. That data then could be mined
20 by these third parties.

21 55. All the methods of monetizing social data were based on selling that data, but such data
22 could be packaged, structured, or mined differently depending on the application for which it was being
23 sold. For advertisers, Facebook's network presented advertisers and Facebook itself with entirely new
24 social signals, such as relationships, events, friendships, and granular interests. Movies, music, and books
25 were inherent parts of a user's profile. The amount of information in Facebook's network that could be
26 mined as social data was unprecedented—and Facebook received all that data daily from its millions of
27 users in the United States and worldwide.

FILED UNDER SEAL

56. The data Facebook collected was uniquely social, derived from the engaged interactions and strong identity of Facebook’s users. Twitter, a public-facing social network, loosely enforced identity and never required users to disclose granular details about themselves. Facebook stood alone in this regard, with a clear product emphasis on individuals and their connections to others. In 2010, Google, Yahoo, and the other major online advertising sources competed in an entirely different market—one based on search data. The data Facebook had at its disposal was not fungible with search data—it was actionable data about individual users, with their identities fully ascertainable.

57. By 2010, Facebook stood alone as the dominant player in the newly emergent market for social advertising—a market in which Facebook’s own users provided Facebook with a constant stream of uniquely valuable information, which Facebook in turn monetized through the sale of advertising. Advertisers, finding no substitute from any other company, paid top dollar for Facebook’s powerful targeting and actionable data, and some of those advertisers—wittingly or not—even fed crucial data about themselves, their products, and the efficacy of their targeting back to Facebook’s network.

58. As Facebook itself explained to third-party developers in May 2007, Facebook’s core value proposition and business model was (a) “providing access to a new kind of data—social data, which enables you to build applications that are relevant to users.” With respect to that data, Facebook told developers: “You are on a level playing field with us. You can build robust apps, not just widgets. Complete integration into the Facebook site.” By 2010, it was clear that Facebook’s entire business was selling this new form of “social data” (and machine-learning-driven user targeting based on that data) and that it would do so by selling access to developers and selling advertisements targeting Facebook’s network of engaged and active users.

C. The Data Targeting Barrier to Entry

59. As Facebook’s dominant position emerged in 2010, powerful network effects and feedback loops took hold and solidified that position. Data provided by users, and user targeting based on that data, made Facebook’s network more valuable, thereby attracting more users to the network. As a typical use case, a Facebook user would invite his closest friends and family, who would then invite

FILED UNDER SEAL

1 and engage with other friends and family members who existed on the network. A familiar feedback
2 loop—a virtuous circle—emerged, rapidly growing Facebook’s user base.

3 60. The content generated by this user base, in turn, increased the value of the Facebook
4 network. With each photograph, relationship status, check-in, or post by a Facebook user, the Facebook
5 network became more valuable, not just as a means of communicating with directly connected
6 acquaintances, but as a means of learning about more remotely connected ones.

7 61. As Samuel Lessin, then Facebook’s VP of Product Management, explained to Mark
8 Zuckerberg in an internal email on October 26, 2012, the data Facebook collects makes Facebook
9 progressively more proficient at collecting and monetizing data:

10 One of the things that puts us currently in a very defensible place is the
11 relationship we have created between the people using Facebook all the
12 time, and us having the information we need to make Facebook a better
13 product. This is the fundamental insight in something like coefficient. *We*
14 *know more about what people want to see because people look at more*
15 *stuff on our platform.* In this respect, while there are other ways to get
close, it feels viscerally correct that there is an ROS dynamic at play, *the*
more people that use the system, the more information we have on how
to make more people use the system.

16 (emphasis added).

17 62. A barrier to entry emerged from this feedback loop. To compete with Facebook, a new
18 entrant would have to rapidly replicate both the breadth and value of the Facebook network—a task a
19 mere clone of that network could not accomplish. Indeed, to compete with Facebook, a competitor would
20 not only have to build its own vast network but would have to draw active social engagement on a massive
21 scale—which likely would require drawing a vast quantity of Facebook users away from that platform.

22 63. The costs to switch would be massive: an entrant-competitor would have to present an
23 overall value proposition to users that not only exceeded that of Facebook’s entrenched network, but did
24 so handily. Moreover, to compete with Facebook’s virtuous circle, the value delivered by an entrant-
25 competitor platform would have to facilitate social data mining, including through machine learning and
26 artificial intelligence, that would create even more value for users, developers, and advertisers. This
27 barrier to entry is referred to throughout this Complaint as the Data Targeting Barrier to Entry (“DTBE”).
28

FILED UNDER SEAL

64. The DTBE protects Facebook's ability to control and increase prices in the Social Advertising Market without the pressures of price competition from existing competitors or new entrants. Because of its monopoly power in the Social Advertising Market and the DTBE, Facebook has been able

Figure 1: Retail Facebook CPM, Q4 2012 – Q4 2013



to consistently increase the price it charges for social advertising. And this is exactly what Facebook has done since it obtained its dominant position in 2010.

65. From 2011 to 2012, for example, Facebook massively increased the prices it charged for its advertisements—one of the primary sales channels for its social data. That year, costs per thousand impressions (CPM) on Facebook increased by 41%, with a 15% increase in the last quarter of 2011 alone. Cost per click (CPC), which is a measure of advertising costs paid on a by-click basis, rose 23% that same year. Facebook increased prices for social advertising as it also grew the number of advertisements it displayed on its site, indicating monopoly power in the Social Advertising Market.

66. Facebook maintained that power over its prices through 2013, with a 2.9x increase in CPMs year over year. The increase came as overall advertising revenues increased yet again—that year by a staggering 83% over the last.

67. These price increases would not be possible without the DTBE. If a rival network existed with comparable social data available for sale through advertising, Facebook's price increases would have been met with customer migration to the comparable rival. But Facebook had no such rival and was unfettered in its ability to increase prices, even while rapidly increasing its supply of data for sale through advertisement.

FILED UNDER SEAL

68. Once Facebook had achieved dominance in the Social Advertising Market, its position only improved—and became more entrenched. The more advertising Facebook sold, and the more social data Facebook collected and packaged for sale, the more effective Facebook became at selling advertising, targeting users, and commercializing direct access to its users’ social data (e.g., through APIs). This, in turn, made entry by a new rival impossible or prohibitively costly, thereby allowing Facebook to increase prices and make additional investments that deepened the DTBE moat surrounding its business.

D. Google’s Failed Entry into the Social Advertising Market

69. In 2010, Google became desperate to enter the Social Advertising Market. It had tried several times to do so before, but each foray was met with failure. Google’s Orkut social network, which was launched days before Facebook, was quickly overtaken. Wave, Google’s social communication platform, never achieved any traction with users. And Google’s Buzz social network—built on the back of its highly successful Gmail product—imploded quickly in early 2010.

70. Google’s next attempt to enter the market attacked Facebook’s functionality head-on, which meant attempting to penetrate the powerful DTBE protecting Facebook’s business. Google made a massive, unprecedented investment of resources into building a product with enough value to lure users away from Facebook’s broad, highly engaged social network.

71. In 2010, Google’s Vic Gundotra became the company’s Chief Architect. Gundotra pitched a new social network to Larry Page, Google’s cofounder, who returned as CEO of the company in 2011. Gundotra repeated an ominous refrain, “Facebook is going to kill us. Facebook is going to kill us,” which frightened Page into action.

72. Page greenlit a new product, Google+. Initially, Google+ sought to leverage Google’s YouTube product to build its social network, requiring a Google+ account for access to certain key features of YouTube. In the face of significant user resistance, Google backed away from that requirement. Nonetheless, Google attempted, through Google+, to build out a “social graph” that would leverage a common user identity across Google products, including YouTube and Gmail.

FILED UNDER SEAL

73. In early 2011, Google began what insiders now refer to as “the 100-day march” toward launch of Google+. The product Google planned to deliver was, by any fair account, uncannily similar to what Facebook offered in terms of product features and functionality. By the summer of 2011, the planned features for Google+ included a continuous scroll product called the “stream” (a clone of Facebook’s “feed” product); a companion feature called “sparks,” which related the “stream” to users’ individual interests; and a sharing app called “Circles,” a purportedly improved way to share information with one’s friends, family, contacts, and the public at large.

74. Unlike Google’s past products, Google+ was not designed to organically grow and scale from small beginnings. From the outset, Google invested massive amounts of resources to bring a finished, full-scale social network to market. Calling the project “Emerald Sea,” Google conscripted almost all of the company’s products to help build Google+. Hundreds of engineers were involved in the effort, which remained a flagship project for Page, who had recently reassumed the Google CEO role. Google’s Gundotra was quoted explaining that the product that would become Google+ was a transformation of Google itself: “We’re transforming Google itself into a social destination at a level and scale that we’ve never attempted—orders of magnitude more investment, in terms of people, than any previous project.”

75. The amount of resources Google brought to bear stood in stark contrast to its previous attempts at penetrating the Social Advertising Market. Google had dedicated barely a dozen staff members to its previous failed social network product, Buzz. At its peak, Google+ involved 1,000 employees from divisions across the country. Google, for example, ripped out its elaborate internal video conferencing system and forced employees to use the Google+ Hangouts video chat feature, which one internal employee described as “janky.” Employee bonuses were tied to the success of Google+. And the entire project was confined to a level of secrecy never before seen at Google.

76. Google+ was released on June 28, 2011. The product included the “stream,” the “Circles” app, the “Hangout” video chat and messaging product, and a photo sharing product. The resemblance to Facebook was striking. As one internal Google employee commented: “this looks just like Facebook. What was the big deal? It’s just a social network.” Another Google employee was quoted as saying, “All

FILED UNDER SEAL

1 this fanfare and then we developed something that in the end was quite ordinary.” One thing was
2 indisputable: with the release of Google+, Google had challenged Facebook head-on by effectively
3 cloning Facebook’s product.

4 77. Because Google’s user base was already massive, the Google+ product attracted millions
5 of users shortly after launch. But though these users signed up for Google+, Google quickly found out
6 they were not using the product. As one former Google employee explained:

7 It was clear if you looked at the per user metrics, people weren’t posting,
8 weren’t returning and weren’t really engaging with the product. Six months
9 in, there started to be a feeling that this isn’t really working.

10 78. The problem for Google+ was the powerful network effect that reinforced the DTBE that
11 protected Facebook. Google’s clone of Facebook did not present enough new value to overcome massive
12 network-based switching costs—the cost to Facebook users of shifting away from an existing networked
13 product in which the users had actively invested their social data for years.

14 79. Paul Adams, a former Google+ user-experience team member, summed it up succinctly
15 when asked why Google+ had failed:

16 What people failed to understand was Facebook and network effects. . . .
17 It’s like you have this grungy night club and people are having a good time
18 and you build something next door that’s shiny and new, and technically
19 better in some ways, but who wants to leave? People didn’t need another
20 version of Facebook.

21 80. By 2014, Google+ was declared a failure and Gundotra, its founder, eventually left
22 Google. Within just a few years, Google—with all of its resources, developers, and existing user base—
23 failed entirely to overcome the DTBE protecting Facebook. As long as Facebook controlled the data
24 derived from an engaged and active user base, it could continue to keep that user base active and engaged.

25 81. The only way to disrupt this virtuous circle was with a rival product that provided
26 significantly more or different value than Facebook, and that itself was propelled to scale by powerful
27 network effects.
28

FILED UNDER SEAL**II. A THREAT TO FACEBOOK'S MONOPOLY: THE RISE OF SMARTPHONES AND MOBILE APPS****A. The Mobile App Revolution**

82. In 2009 and 2010, as Facebook emerged the undisputed winner of the social media wars, another new market had begun to take hold. The launch of the Apple iPhone in 2007 created a market for a new type of cellular phone: one with a user interface capable of robust Internet connectivity and messaging. No longer constrained by numeric keypads for texting—or clunky, permanent alphanumeric keyboards attached to phones, such as with the Treo or Sidekick cellular phones—the iPhone dynamically displayed a multi-touch keyboard and came equipped with a full-featured web browser that rendered complete web pages.

83. By the summer of 2008, Apple's newest iPhone, the iPhone 3G, was released with onboard GPS and other hardware upgrades. Accompanying the release of the new iPhone was a new store for third-party applications that would run natively on the iPhone: the Apple App Store, which opened for business on July 10, 2008, the day before the release of the iPhone 3G.

84. Developers who launched their third-party applications via the App Store reaped huge rewards. There were approximately 500 apps available at the App Store's initial launch. Games using the iPhones accelerometer became immediate successes, some quickly earning hundreds of thousands of dollars by selling downloads for just a few dollars each. Applications that exploited the new GPS functionality in the iPhone also quickly became popular. By September 2008, the Apple App Store had racked up 100 million downloads, and by 2009, it hit 1 billion. iPhone apps had become a new means to deliver scaled value to countless users. Google also launched what became its Play Store (initially known as Android Market) in 2008. It soon overtook Apple's App Store in terms of overall volume, with 82% growth. The mobile app revolution had begun.

85. Mobile apps rapidly proliferated, with huge opportunities for further growth—as the lion's share of cell phone activity by 2010 had become something other than making phone calls. For example, a 2010 Pew Research survey showed that taking pictures and sending text messages had become the most common uses for cellular phones among adults, with more than a third of adult cell phone users accessing

FILED UNDER SEAL

the Internet, playing games, emailing, recording video, or playing music through their cell phones. At the same time, 29% of adult cell phone users had used a downloaded app.

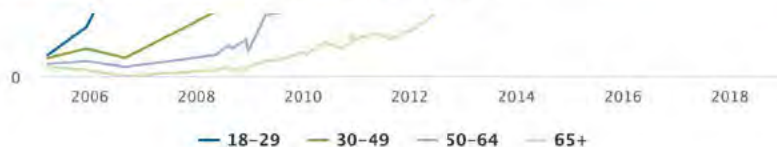
86. A 2010 Nielsen survey showed that games, news/weather, maps and navigation, and social networking were the most popular apps on cellular phones.

87. Notably, mobile apps resonated most strongly with the demographics that had recently adopted social media and were providing their data to Facebook in droves. App users among cell phone

% of adult cell phone users who do each of the following on their phone...

| | |
|----------------------------------|-----|
| Take a picture | 76% |
| Send or receive text messages | 72 |
| Access the internet | 38 |
| Play a game | 34 |
| Send or receive email | 34 |
| Record a video | 34 |
| Play music | 33 |
| Send or receive instant messages | 30 |
| Use an app | 29 |

Source: Pew Research Center's Internet & American Life Project, April 29-May 30, 2010 Tracking Survey. N=1,917 adult cell phone users.



Source: Surveys conducted 2005-2019.

PEW RESEARCH CENTER



Source: The Nielsen App Playbook, December 2009. N=3,962 adults who have downloaded an app in the 30 days prior to the survey.

FILED UNDER SEAL

owners were disproportionately younger, with 44% of app users in 2010 under the age of 20 and another 41% between the ages of 30 and 49. These were the same demographics that were rapidly adopting social media as part of their lives and providing Facebook with the social data that built and maintained the DTBE that protected its business.

88. Many of the mobile apps that were rapidly attracting users were doing so because they presented their own specialized value propositions. These apps had to be specialized because cellular phone screens were smaller, particularly in 2010, and mobile traffic was driven by specialty software, often designed for a single purpose. Users signed up for these apps with their e-mail addresses and personal information and interacted directly with the apps.

89. As *Wired* magazine described in 2010, a typical user moved from app to app, each with some specialized use:

You wake up and check your email on your bedside iPad—that's one app. During breakfast you browse Facebook, Twitter, and the New York Times—three more apps. On the way to the office you listen to a podcast on your smartphone. Another app. At work, you scroll through RSS feeds in a reader and have Skype and IM conversations. More apps. At the end of the day, you come home, make dinner while listening to Pandora, play some games on Xbox Live, and watch a movie on Netflix's streaming service.

90. In 2010, Morgan Stanley projected that within five years, the number of users who accessed the Internet from mobile devices would surpass the number who accessed it from PCs. The Internet was at an inflection point—the World Wide Web was no longer the dominant way to access information. Users were obtaining their information from specialized walled gardens, and Facebook's own walled garden was one app away from being superseded.

91. The years leading up to 2010 saw the rise of streaming apps, such as Netflix and Pandora, and e-book readers, such as Kindle and iBooks. Apple's 2010 list of top-grossing iPhone apps included mobile games such as Angry Birds, Doodle Jump, Skee-Ball, Bejeweled 2 + Blitz, Fruit Ninja, Cut the Rope, All-in-1 GameBox, the Moron Test, Plants vs. Zombies, and Pocket God. Facebook's mobile app

FILED UNDER SEAL

1 topped the list of free downloads in the App Store, along with Words with Friends, Skype, and the
2 Weather Channel App.

3 **B. Facebook Recognizes the Looming Threat Presented by Mobile Applications**

4 92. By 2011, Facebook realized that it had fallen behind. Facebook had just debuted its new
5 “Timeline” product, a controversial modification of the Facebook feed that generated dynamic content
6 for each user rather than a static series of posts visible to the user. Facebook had spent the last eight
7 months prioritizing its desktop experience and its new Timeline product. But while it did so, mobile
8 applications continued their meteoric rise.

9 93. Facebook’s own mobile application was built on a technology called HTML5, which at
10 the time was good for building web pages but not for building mobile apps native to iOS and Android
11 smartphones. As a result, Facebook’s mobile app was buggy, prone to crashes, and painfully slow. As
12 Zuckerberg would lament years later about HTML5, “We took a bad bet.”

13 94. Zuckerberg reflected in 2018 that Facebook had fallen behind when mobile apps emerged:

14 One of my great regrets in how we’ve run the company so far is I feel like
15 we didn’t get to shape the way that mobile platforms developed as much as
16 would be good, because they were developed contemporaneously with
17 Facebook early on. I mean, iOS and Android, they came out around 2007,
18 we were a really small company at that point—so that just wasn’t a thing
19 that we were working on.

20 95. As mobile apps rose, Facebook’s desktop product acquired users at a slower pace. All of
21 this occurred as Facebook was planning its initial public offering. Facebook knew that its position was
22 eroding and that if mobile growth continued, its IPO debut would be in the midst of material changes to
23 its business, undermining Facebook’s financial and qualitative disclosures to public investors.

24 96. But there was no avoiding the issue. Facebook held its IPO on May 18, 2012. By the time
25 Facebook released its first annual report, the trend was unmistakable—the transition to mobile devices
26 from desktop web-based applications posed an existential threat to Facebook’s business. In its 2012 Form
27 10-K, Facebook disclosed this risk to shareholders as one of the factors that affected its bottom line:
28

FILED UNDER SEAL

Growth in the use of Facebook through our mobile products as a substitute for use on personal computers may negatively affect our revenue and financial results.

We had 680 million mobile MAUs in December 2012. While most of our mobile users also access Facebook through personal computers, we anticipate that the rate of growth in mobile usage will exceed the growth in usage through personal computers for the foreseeable future and that the usage through personal computers may decline or continue to decline in certain markets, in part due to our focus on developing mobile products to encourage mobile usage of Facebook. For example, during the fourth quarter of 2012, the number of daily active users (DAUs) using personal computers declined modestly compared to the third quarter of 2012, including declines in key markets such as the United States, while mobile DAUs continued to increase. While we began showing ads in users' mobile News Feeds in early 2012, we have generated only a small portion of our revenue from the use of Facebook mobile products to date. In addition, we do not currently offer our Payments infrastructure to applications on mobile devices. If users increasingly access Facebook mobile products as a substitute for access through personal computers, and if we are unable to continue to grow mobile revenues, or if we incur excessive expenses in this effort, our financial performance and ability to grow revenue would be negatively affected.

C. The Facebook Platform

97. Although Facebook faced a looming threat from mobile applications, it maintained an important source of leverage: its social data. Facebook possessed (and continued to receive) vast quantities of information about its massive user base, including how each user was connected to others. This information was valuable to both new and existing mobile applications, which could leverage Facebook's social data to obtain new users and to build novel social features, functions, and apps.

98. Facebook referred to its network as its "Graph," coined after a mathematical construct that models connections between individual nodes. The Facebook Graph contained user "nodes," with connections and information exchanged among nodes as "edges." Facebook coined the term "Open Graph" to describe a set of tools developers could use to traverse Facebook's network of users, including the social data that resulted from user engagement.

FILED UNDER SEAL

1 99. Importantly, Open Graph contained a set of application programming interfaces (“APIs”)
2 that allowed those creating their own social applications to query the Facebook network for information.
3 As Facebook explained in its 2012 Form 10-K:

4 ***Open Graph.*** Our underlying Platform is a set of APIs that developers can
5 use to build apps and websites that enable users to share their activities with
6 friends on Facebook. As Open Graph connected apps and websites become
7 an important part of how users express themselves, activities such as the
8 books people are reading, the movies people want to watch and the songs
9 they are listening to are more prominently displayed throughout
Facebook’s Timeline and News Feed. This enables developer apps and
websites to become a key part of the Facebook experience for users and
can increase growth and engagement for developers.

10 100. Open Graph, along with other Facebook products, such as its NEKO advertising and
11 Payments products, comprised Facebook’s Platform. The Platform was vital to Facebook’s business
12 because it ensured that engagement continued on Facebook. Without the Platform, Facebook would be
13 required to build applications that increased the value of its network itself—meaning that Facebook would
14 have to try to predict what applications users wanted; design, code, and scale those applications across
15 its user base and network; and bear the risk and resource drain of guessing wrong and making mistakes.

16 101. Facebook did not have the resources to do this, so it decided instead to allow third parties
17 to build applications for the Platform. As Mark Zuckerberg observed in a February 2008 email to
18 Facebook’s VP Engineering for Platform Michael Vernal, a senior Zuckerberg lieutenant who was in part
19 responsible for creating Open Graph:

20 Platform is a key to our strategy because we believe that there will be a lot
21 of different social applications And we believe we can’t develop all
22 of them ourselves. Therefore It’s important for us to focus on it
23 because the company that defines this social platform will be in the best
position to offer the most good ways for people to communicate and
succeed in the long term.

24 102. Put simply, Facebook could either speculate on new social applications by building them
25 itself or it could provide a platform for others to do so. For years, Facebook opted to provide a platform
26 until it was able to develop its own social applications.

FILED UNDER SEAL

1 103. But Facebook also recognized that developers on its Platform could potentially pose a
2 competitive threat. In its 2012 annual report, Facebook disclosed the following significant risk factor to
3 its operations:

4 In addition, Platform partners may use information shared by our users
5 through the Facebook Platform in order to develop products or features that
6 compete with us. . . . As a result, our competitors may acquire and engage
7 users at the expense of the growth or engagement of our user base, which
8 may negatively affect our business and financial results.

9 104. Thus, Facebook knew that competition could come from its own third-party application
10 developers. But Facebook nevertheless actively sought developers to build applications on its Platform
11 because of the potential to extract profits from the applications these developers built and the users they
12 attracted to, and engaged on, Facebook's network.

13 105. As Facebook explained to its investors in 2012, maintaining a Platform on which
14 developers could build applications meant more engagement and therefore greater ad revenues for
15 Facebook:

16 Engagement with our Platform developers' apps and websites can create
17 value for Facebook in multiple ways: our Platform supports our advertising
18 business because apps on Facebook create engagement that enables us to
19 show ads; our Platform developers may purchase advertising on Facebook
20 to drive traffic to their apps and websites; Platform developers use our
21 Payment infrastructure to facilitate transactions with users on personal
22 computers; Platform apps share content with Facebook that makes our
23 products more engaging; and engagement with Platform apps and websites
24 contributes to our understanding of people's interests and preferences,
25 improving our ability to personalize content. We continue to invest in tools
26 and APIs that enhance the ability of Platform developers to deliver
27 products that are more social and personalized and better engage people on
28 Facebook, on mobile devices and across the web.

106. Facebook's Platform was valuable to Facebook in several important ways.

107. First, the Platform meant that new applications would be built on Facebook's network,
increasing the value of Facebook's network as the applications became more popular. The increased
engagement with Facebook as a result of these new applications translated to better-targeted content and
higher advertising revenues.

FILED UNDER SEAL

108. Second, Facebook would not need to spend significant resources to develop new applications or test new business models—third parties would do that instead. Facebook could merely wait for an application built for its Platform to gain widespread adoption, then either build a competing application or passively glean the benefits of that popular application’s user engagement, including valuable new social data for Facebook and its network.

109. Third, access to Facebook’s network was itself valuable to third-party developers, so Facebook could charge developers—most notably, through API access and advertising purchases—to access Facebook’s Platform and the social data it collected from Facebook’s massive number of engaged users.

D. The Profitable Open Graph Platform and Mobile Install Business

110. Facebook continued to struggle to catch up with the new onslaught of mobile applications, but it recognized that the new apps required aggressive user growth to be profitable. Among other things, Facebook’s APIs allowed mobile app developers to query the friends of a person’s friends, which allowed mobile applications to find other users who might be interested in using their apps.

111. Mobile apps also could use Facebook to communicate across Facebook’s network, either directly with a user’s friends or with others not directly connected with the user. A mobile payment application, for example, could enable two strangers to pay each other, even if they were not directly connected on Facebook—so long as both of them existed somewhere on Facebook’s Platform. A user of a dating application, such as Tinder, could use Facebook’s APIs to find a compatible date, either in the extended network of one’s friends or beyond—anywhere on Facebook’s Platform.

112. Facebook quickly realized it could monetize the value of its network through third-party mobile applications, and it moved aggressively to do so, beginning with games built to run on Facebook’s Platform. Those games, many of which were social games that allowed users to play with and against each other, sought above all else new users to increase their adoption. Facebook’s Vernal sought to obtain a beachhead with these applications, monetizing each additional game install that resulted from the use of Facebook’s Platform or from Facebook’s advertising product, NEKO.

FILED UNDER SEAL

113. For example, Facebook included ads as “stories” on user timelines that indicated whether the user knew other users who were playing a particular game. Facebook then monetized such advertisements when the game obtained new users from them. As Vernal explained in a May 2012 e-mail:

The biggest/most efficient market segment for advertising on mobile today is driving app installs. This is at least partly because it’s the most measurable—if you know that you get \$0.70 from every game you sell, then in theory you can afford to pay up to \$0.69/install. This kind of measurability allows for maximal bidding.

So, what we’re trying to do is kickstart our sponsored stories business on mobile by focusing on one particular type of story (is-playing stories) and one market segment (games), make that work really well, and then expand from there.

114. Facebook thus leveraged its most valuable asset—the information it had about its users, their interests, and most importantly, their friends—to make money from the proliferation of mobile games.

115. Games like Farmville, a mobile application that allowed players to create their own simulated farms, quickly took off because of Facebook’s Platform. Facebook increasingly recognized that it could obtain engagement from users through the game itself.

116. This strategy led to a broader one, in which Facebook drove app installs by allowing developers to advertise to its user base and traverse Facebook’s social network through the Facebook APIs. Facebook collected a fee for each app install that resulted from its network. Vernal outlined the plan in detail:

Roughly, the plan:

1/ Create new iOS + Android SDKs, because the current ones are terrible. Ship Thunderhill so we get even broader adoption of our stuff.

2/ Wire them up to make sure we know when you’re playing a game (so we can generate the same kind of is-playing stories we can on canvas).

3/ Generate a bunch of effective, organic distribution for these games via our existing channels (news feed, net ego on both desktop + mobile). Ship

FILED UNDER SEAL

1 send-to-mobile, which allows us to leverage our desktop audience to drive
2 mobile app traffic.

3 4/ Create an even better app store than the native app stores (our app center)
4 and make a lot of noise about it, so developers know that they should be
5 thinking about us to get traffic to their mobile apps.

6 5/ Introduce a paid offering, probably cost-per-install (CPI) based, where
7 you can pay us to get installs from your mobile app. Primary channels for
8 this paid distribution are News Feed and App Center (on desktop + mobile)
9 as well as RHC on desktop.

10 117. The strategy was clear, not just for gaming, but for mobile apps. Facebook would make
11 money by allowing app developers to leverage its user base. Facebook would advertise social games to
12 its users by plumbing their social data—including data about when they played games and which of their
13 friends played them—and in exchange, Facebook would receive some amount of money per install, which
14 would be the app developer's cost-per-install (CPI). The same plan would work for mobile applications
15 generally.

16 118. By the end of 2011 and the beginning of 2012, Facebook began discussing other ways to
17 monetize its Platform, including its Open Graph APIs. One way was to sell API access based on usage.
18 Zuckerberg and top executives at Facebook extensively debated a tiered approach to API access.
19 Facebook deliberated over a pricing model for API access, and internally decided that it would be possible
20 to sell API access to third-party developers. Facebook also decided that it could bundle API access with
21 the ability to advertise on Facebook. However, as explained below, Facebook gave up the profits it could
22 glean from API access for the chance to dominate the Social Advertising Market entirely, excluding
23 competitors (both actual and potential) and leveraging network effects to achieve and maintain monopoly
24 power.

25 **III. FACEBOOK WEAPONIZES ITS PLATFORM TO DESTROY COMPETITION**

26 **A. Facebook Makes Plans to Remove Vital Platform Functionality and Refuses to Sell**
27 **Social Data to Competing Application Developers**

28 119. Although Facebook had made significant amounts of revenue and profit selling access to
its social data through its APIs and its NEKO advertising system and had planned to expand that business,
it chose not to, sacrificing those significant profits.

FILED UNDER SEAL

1 120. By the end of 2011 and the beginning of 2012, Zuckerberg along with Facebook’s Vice
2 President of Growth, Javier Olivan, its VP of Product Management, Samuel Lessin, and Michael Vernal
3 internally debated a plan to prevent third-party developers from building their own competing social
4 networks that could be capable of generating engagement and social data independent of Facebook’s
5 Platform.

6 121. Emerging mobile applications such as Line, WeChat, and Instagram were creating their
7 own vast user bases with identity and login features separate from the Facebook Platform. Their
8 increasing ubiquity posed an existential threat to Facebook’s core business, which relied heavily on
9 engagement from its user base. These applications provided quintessentially social applications, such as
10 image sharing, messaging, and payments—a direct threat to Facebook’s own applications, including
11 Facebook’s own fledgling Messenger application.

12 122. Mobile applications were rapidly eating away at Facebook’s dominance, which relied
13 heavily on its web-based desktop product. Zuckerberg openly acknowledged that its desktop applications
14 were not the future and that native phone apps would dominate the mobile web in the future.

15 123. Zuckerberg therefore sought to consolidate core applications into its own centralized
16 Facebook application, noting in a March 2012 Q&A with employees that Facebook was “building
17 towards social Facebook versions where you can use the individual app or the Facebook version.” That
18 is, users could “replace whole parts of your phone with these Facebook apps and [they] will be a whole
19 package for people.”

20 124. Beginning in the fall of 2011 and well into 2012, Mark Zuckerberg and his chief
21 lieutenants, Lessin and Vernal, planned to address the looming mobile applications threat. Their solution
22 was a scheme to disrupt the massive growth of mobile applications by attracting third-party developers
23 to build for Facebook’s Platform and then remove their access to the APIs that were most central to their
24 applications. They would accomplish this by leveraging Facebook’s “Friends” and “Timeline” APIs, as
25 well as other vital APIs, including those relating to messaging.

26 125. The Friends APIs let third-party developers traverse the Facebook Graph, searching
27 through a user’s friends as well as the friends of their friends. Zuckerberg and his executives proposed
28

FILED UNDER SEAL

1 modifying the APIs to deny third-party developers access to information about a user's friends (and the
2 friends of their friends) unless that developer's application was already installed by a user's friends to
3 begin with. This ensured that new applications could not obtain new users or use Facebook's social data
4 to increase the value of their application.

5 126. Facebook also foreclosed developers from continuing to extract information about a user's
6 friends from their timeline or news feed. Thus, third-party applications that relied on the stream of
7 information that flowed through a user's news feed, such as a post about a friend of the user getting
8 engaged or sharing a news article, would be abruptly left with none of the social data they needed to
9 function.

10 [REDACTED]
11 [REDACTED]
12 [REDACTED]

13 128. Removing access to these APIs halted the growth of tens of thousands of third-party
14 applications that relied on these essential APIs and were, in Facebook's view, threatening Facebook's
15 dominance by eroding the DTBE that protected Facebook's business.

16 129. Facebook's plan prevented any competitive third-party application from buying social
17 data from Facebook, either through its Platform APIs or through its advertising Platform. As Vernal
18 explained to Lessin in August of 2012, Facebook would "not allow things which are at all competitive to
19 'buy' this data from us."

20 130. Facebook thus refused to sell its social data to any competitive third-party developer,
21 sacrificing significant short-term profits in exchange for a competitive advantage in the Social
22 Advertising Market. If not for the prospect of driving these competitors out of the markets in which
23 Facebook competed, the decision to refuse to sell social data to third-party developers made no economic,
24 technical, or business sense.

25 131. Third-party developers with successful applications increased the value of Facebook's
26 overall network by increasing engagement and generating the very social data Facebook sold through its
27 targeted advertising channels, including to developers. As Zuckerberg had observed years earlier,
28

FILED UNDER SEAL

Facebook itself could not broadly develop new third-party apps or anticipate what apps would be successful, so it relied on third parties to do so. Refusing API and social data access to third parties meant that they could not develop the applications that were vital to Facebook’s growth, engagement, and advertising revenue. Facebook decided to deliberately sacrifice the value its third-party developers provided to secure dominance in the Social Advertising Market.

B. Facebook’s Social Data Heist

132. In May 2012, Zuckerberg decided to use the threat of blacklisting from its Platform to extract precious social data from some of Facebook’s competitors. He instructed his executives to quietly require “reciprocity” from major competitors that used Facebook’s Platform. The reciprocity Zuckerberg demanded was the very lifeblood of these competitors’ businesses—the social data harvested from user engagement on their competing networks.

133. By the middle of 2012, Facebook began to block some of its competitors from using its Platform and thereby obtaining Facebook’s social data. Facebook had already blocked Google, including its competing social network Google+, from access to Facebook’s APIs and advertising platform. With respect to Twitter, Instagram, Pinterest, and Foursquare, Facebook would demand “reciprocity” or blacklist them. Reciprocity, of course, meant that these competing social networks would have to hand over their most valuable asset—their social data—to their rival Facebook.

134. If rivals did not comply with Zuckerberg’s demands to hand over their social data to Facebook, Facebook would simply take it. In May 2012, Vernal directed his subordinates, Douglas Purdy (Director of Engineering for Platform) and Justin Osofsky (VP of Global Operations), to build “our own hacky scraper” and a “bunch of scrapers” to crawl rival sites like Twitter and Instagram and harvest their social data—with or without their consent. If Twitter or Instagram refused to agree to Zuckerberg’s “reciprocity” proposition, Facebook would use the scrapers to obtain the data instead.

135. In August 2012, Facebook considered broadening its list of companies to shake down for social data—or to block entirely from Facebook’s Platform. That month, Facebook’s then VP of Business and Marketing Partnerships, David Fischer identified other potential product categories and competitive companies in each category to block:

FILED UNDER SEAL

I'd expect that a large part of the market for our network will come from current and potential competitors. Here's the list that Jud worked up of what we'd likely prohibit if we were to adopt a ban on "competitors" using a broad definition:

- Social network apps (Google+, Twitter, Path, etc.)
- Photo sharing apps (Picasa, Flickr, LiveShare, Shutterfly, etc.)
- Messaging apps (WhatsApp, Viber, Imo, KakaoTalk, etc.)
- Local apps (Google+ local, Google Offers, Yelp, yp, etc.)
- Social search apps (HeyStaks, Wajam, etc.)
- Platforms (Google Play, Amazon, etc.)

136. Facebook thus identified its direct, horizontal competitors for social data, including those competitors that had, or could create, rival social advertising platforms. These categories of competing applications, particularly on mobile platforms, threatened Facebook's business because they created social networks independent of Facebook, each capable of generating their own valuable social data. If Facebook lost control over these companies, it would lose access to the social data they generated, which meant Facebook's own product could not drive engagement and sell advertising. This was because Facebook's machine-learning algorithms—used to target users for advertising and content, including by granular demographics—required social data to function.

137. In August 2012, Facebook gave a presentation to its Board of Directors that included various revenue models to monetize its Platform, including its APIs. The Board understood that Facebook could monetize its Platform by charging per company, per application, per user, or per API call.

138. But Facebook opted to do none of those things. Instead, it decided to sacrifice those profits in the short term to obtain complete control over the growing mobile application and advertising markets, thereby maintaining and furthering its dominance of social data and the Social Advertising Market.

139. Facebook's plan was to instead block competitors from using its Platform, thereby preventing them from eroding the DTBE that protected Facebook's business. In the case of a select few companies with social data that Facebook needed to maintain and grow its own business, however, Facebook would coerce them into agreements to share their most valuable social data with Facebook. If

FILED UNDER SEAL

1 they refused, Facebook would blacklist them and take it from them anyway with its own crawling
2 software that would scrape their public-facing site for information.

3 140. In September 2012, Zuckerberg formalized his order to shut down the Friends and News
4 Feed/Timeline APIs and to coerce rivals into providing their valuable data to Facebook on pain of
5 blacklisting. On October 30, 2012, Vernal notified his subordinates of Zuckerberg's decision:

6 We are going to dramatically reduce the data we expose via the Read API
7 We are going to change friends.get to only return friends that are also
8 using the app Since friends.get will only return other TOSed users'
9 data [data from users that agreed to an application's terms of service], that
10 means we no longer need the friends_* permissions. We are going to
11 remove/whitelist access to the Stream APIs [the News Feed API]. We are
going to limit the ability for competitive networks to use our platform
without a formal deal in place We are going to require that all platform
partners agree to data reciprocity.

12 141. This decision meant several things: (1) when a third-party application called the Friends
13 APIs, it could not obtain information about a user's other friends unless those friends already had installed
14 the application; (2) the News Feed APIs would no longer provide information about a user's connections;
15 (3) access to those API could be "whitelisted" for third-party developers that were offered—and agreed
16 to—data reciprocity; and (4) reciprocity would be required for any access to the APIs.

17 142. In November 2012, Osofsky, who was then head of Facebook's Platform, summarized the
18 policy changes required by the decision:

19 Policy changes: define competitive networks + require they have a deal
20 with us, regardless of size. Maintain size-based thresholds for all other
21 developers to force business deals. Require data reciprocity for user
extended info to ensure we have richest identity.

22 143. Facebook knew that these changes would eliminate the "growth channel used by 23% of
23 all Facebook apps" and that 89% of the top 1,000 iPhone apps relied on the full friends list API, with
24 75% of the top 1,000 iPhone apps relying on the Friends permissions APIs. Facebook determined that
25 popular applications on its platform with millions of customers would break as a result of the decision,
26 including FarmVille, ChefVille, CityVille, Skype, Spotify, Xobni, Texas Holdem, Yahoo, Trip Advisor,
27 Microsoft's Birthday Reminders, Samsung's clients, Glassdoor and dozens of others.
28

FILED UNDER SEAL

1 144. On November 19, 2012, Zuckerberg broadly announced his decision to block competitors
2 or require full data reciprocity for continued access. Facebook's COO Sheryl Sandberg immediately
3 ratified the decision, adding that "we are trying to maximize sharing on Facebook, not just sharing in the
4 world," with the note that the distinction was a "critical one" and the "heart of why."

5 145. Facebook began preparing its 2013 plan for its mobile advertising business, which
6 included the launch of a new version of its Platform, version 3.0. Platform 3.0 would (according to
7 Facebook) facilitate Facebook's transition from its desktop advertising business to a mobile advertising
8 business. A central element of the transition plan was the implementation of Zuckerberg's decision to
9 remove the Friends and News Feed APIs.

10 146. Vernal explained Zuckerberg's decision to other Facebook employees in November 2012,
11 noting that he believed the amount of data that Facebook required from competitors was "crazy":

12 [A company must share] every piece of content by that user that can be
13 seen by another user. What Mark is saying is he wants certain partners (I
14 assume not all) to give us news feeds on behalf of their users, which is kind
 of crazy.

15 147. Facebook continued to formalize its plan to require the right to crawl the sites of its
16 competitors as a condition of access to its Platform. In November 2012, Facebook's Group Product
17 Manager, Rose Yao explained the scheme:

18 We also reserve the right to crawl a partner website for the user's data.
19 Partners cannot blacklist or block Facebook from crawling your site or
20 using the API. If they do, Facebook reserves the right to block the partner
21 from using our APIs The theory behind Action Importers was that we
22 needed to balance the leverage. You can call our APIs and access our data,
23 as long as we can call your APIs (if you have them) or crawl your web site
24 (if not) and access your data. It's one thing to drag your heels, but if we're
25 the ones doing the work then we force you to make a decision—either you
26 allow us access to your data, or you block us. If you block us, then it's
27 really easy/straightforward for us to decide to block you. What's changed?
28 *When we first started discussing this, we were talking about doing this
 only for top partners. I think a lot of folks interpreted this as just a
 negotiation tactic—we'd just threaten to do this if they didn't cooperate.
 What's changed between then and now is that this is now very clearly not
 a negotiation tactic—this is literally the strategy for the read-side
 platform.*

FILED UNDER SEAL

1 (emphasis added).

2 148. Thus, what began as a negotiation strategy to extract social data from rivals became the
3 foundation of Facebook's Platform strategy. For competitors that posed enough of a threat to create their
4 own rival network, Facebook required them to hand over the only leverage they had—the social data they
5 derived from their users' engagement.

6 149. For some rivals that directly competed, no amount of data would justify access to
7 Facebook's Platform, and for nascent threats that relied on Facebook's platform that did not have any
8 useful data to extract, Facebook's decision was to simply cut off their access to the Friends and News
9 Feed APIs, killing their businesses almost immediately.

10 150. Vernal expressed concern about the strategy to Zuckerberg in November 2012, noting that
11 he was skeptical that competitors such as Pinterest would allow Facebook to take their social data. If they,
12 as well as others, did, Facebook would become a central exchange for data collected among competitors.
13 That is, competitors would share the data to Facebook and Facebook would then share that data back to
14 the competitors that participated in the scheme. *Facebook would become a data-passthrough*
15 *mechanism.*

16 151. In December 2012, despite recognizing that API access, particularly when bundled with
17 Facebook's NEKO advertising platform, was profitable, Facebook decided not to charge for API access
18 and began full implementation of Zuckerberg's decision.

19 152. Although Facebook had planned to announce its decision not to allow access to Friends
20 data through its Friends and News Feed APIs in a public blog post, Zuckerberg vetoed that decision in
21 December 2012. Instead, Zuckerberg decided to enforce the decision selectively and covertly after
22 deliberately analyzing Facebook's competitors. Some competitors would be blocked entirely from the
23 APIs, while some select few would be blocked only if they did not provide their own social data to
24 Facebook.

25 **C. Facebook Targets Its Competitors for Reciprocity or Denial of API Access**

26 153. Beginning in January 2013, Facebook began an internal audit of all of the applications that
27 relied on its Platform. It immediately identified competitors to shutdown entirely from accessing
28

FILED UNDER SEAL

Facebook's APIs or advertising platform. Specifically, Zuckerberg ordered that WeChat, Kakao, and Line be restricted from using the Friends and News Feed APIs and even from advertising on Facebook's NEKO and other platforms.

154. Facebook's David Fischer balked at the decision, noting that blocking competitors even from the advertising platform was irrational and unworkable:

I continue to believe we should allow ads from competitors for several reasons: We should be secure enough in the quality of our products to enable them to compete effectively in the open marketplace . . . It looks weak to be so defensive. This will be a challenge to enforce. We have many competitors and the list will grow in time. How will we judge retailers and e-commerce sites as we grow Gifts, since they arguably are competitors too?

155. Fischer was right. The decision made no rational economic or business sense. The sole purpose of refusing to sell social data as part of the Facebook Platform or through advertising was to shut out competition and allow Facebook to dominate the Social Advertising Market. Aside from that anticompetitive purpose, the decision to refuse to sell social data or advertisements even at full price was so facially irrational that Facebook's own employees who may not have been fully privy to the anticompetitive scheme protested at the irrationality of the decision.

156. That same month Facebook's Osofsky pleaded with Vernal to make an announcement that would send a clear signal to developers, but Vernal responded that Zuckerberg had already rejected that approach. As Vernal explained, telling developers about the decision means bearing the "very real cost" of "changing the rules," including the "PR cost" of betraying developers that Facebook had induced to build for Facebook's APIs and Platform.

157. That same month, Facebook continued to implement Zuckerberg's decision to blacklist competitors. He ordered that Facebook competitor Vine be "shut down" from Facebook's API and Platform, including from advertising. Facebook had again sacrificed the profits it would glean from increased engagement and advertising revenue as a result of Vine's use of Facebook's Platform in exchange for the exclusion of Vine from the competitive landscape.

FILED UNDER SEAL

158. Indeed, Facebook’s mobile advertising platform was growing rapidly, and blocking large companies from using it made no economic sense other than to effectuate Zuckerberg’s scheme to prevent rivals from competing with Facebook. In a January 20, 2013 email, Facebook’s then-Director of Product Management and Platform Monetization team, Deborah Liu reported: “Neko grew another 50% this week! Hit a high of \$725k Friday (see charge below). We are now 5% of total Ads revenue and 21% of mobile ads revenue.”

159. Lessin responded to the news: “The neko growth is just freaking awesome. Completely exceeding my expectations re what is possible re ramping up paid products.”

160. Liu was clear, however, that the increased revenues occurred notwithstanding the blacklisting of formerly large spenders, such as WeChat: “WeChat and other competitive networks are no longer advertising on Neko based on policy.”

161. In February of 2013, Facebook shut down Yahoo!’s access to key APIs, resulting in direct negotiations between Yahoo!’s Marissa Mayer and Facebook’s Sheryl Sandberg in order to restore Yahoo!’s access to the Facebook Platform.

162. In March 2013, Facebook’s key Platform employees began to voice concern that the approach taken by Facebook of shutting down access and then coercing “data reciprocity” was problematic. They instead encouraged making an upfront announcement that the APIs would be unavailable and then negotiating a deal for access to Facebook’s Platform. In an e-mail that month from Purdy to other Facebook employees and executives, he wrote:

I have been thinking about the challenges around reciprocity and competitive enforcement (friends.get, etc.) and fact that *it is all post facto*. The way we are structured today, you build an app on FB and then launch and then we may just shut you down, harming users and the developer. I wonder if we should move as quickly as possible to a model in product where all you get from platform is login (basic info) and sharing without approval. All other APIs are available in development, but have to be approved before the app launches to real users (basically all apps using friends.get have to have that capability approved). We are roughly on course to deliver this as part of unified review, save for the more granular approval for things like friends.get? What I love about this too is we could make our whitelists so much cleaner by making each capability an approval thing. Marie: I think makes your “deprecations” much easier. Thoughts?

FILED UNDER SEAL

1 163. Although Facebook moved towards full deprecation of the APIs with the exception of
2 those with whitelisting agreements, it continued its campaign of quietly shutting down competitors'
3 access to the APIs and then asking them to make a reciprocity deal. Indeed, Facebook soon thereafter
4 shut down three competing Amazon apps, resulting in Amazon protesting that the decision “will break 3
5 of our live integrations.”

6 164. That same March in 2013, Facebook used API and Platform access as leverage to acquire
7 rival Refresh.io. Facebook internally decided that it would threaten Refresh.io with denial of access to
8 the APIs unless it sold its business to Facebook. That same form of leverage would be used to acquire
9 other rivals—either they sold to Facebook or they saw their business ejected from Facebook’s Platform.

10 165. In 2013, Facebook also began using mobile spyware company Onavo to secretly track
11 application usage on customers’ phones. Onavo, through deceptive terms of service, tracked app usage
12 in real time, and Facebook used that data to target specific competitors. By April 2013, Olivan was using
13 Onavo to track Snapchat, Pinterest, WhatsApp, Tumblr, Foursquare, Google, Path, vine, Kik, Voxer,
14 MessageMe, Viber, GroupMe, Skype, Line, and Tango. One internal Olivan presentation contained
15 detailed usage data for these applications from August 2012 to March 2013.

16 166. By July 2013, Onavo data was providing detailed intelligence to Facebook on 30 million
17 Onavo users. Among all of the apps, the data showed the meteoric rise of WhatsApp, a direct competitor
18 to Facebook’s own fledgling product, Messenger.

19 167. Armed with detailed intelligence about its competitors—both on and off the Facebook
20 Platform—Facebook ordered a detailed audit of Facebook applications that relied on the Friends and
21 News Feed APIs.

22 168. Facebook’s Director of Developer Platforms & Programs, Konstantinos Papamiltiadis,
23 reported back that there were 40,000 apps using the APIs that were to be restricted, with 7% of them
24 being photo or video sharing apps.

25 169. Facebook then began to categorize these third-party applications into three general
26 categories: (1) developers that “may cause negative press” if their access to APIs were shut down; (2)
27 applications that “provide strategic value”; and (3) applications that were “competitive” or “not useful to
28

FILED UNDER SEAL

1 FB. Application developers that would experience “a Major Business Disruption/Kill” as a result of the
2 restriction of API access received a “PR flag.”

3 170. In response to the categorization, Lessin immediately ordered his subordinates to “shut
4 down access to friends on lifestyle apps . . . because *we are ultimately competitive with all of them.*”
5 (emphasis added).

6 171. As Facebook continued its analysis of the applications that relied on the Friends and News
7 Feed APIs, it became clear that Facebook’s plan would result in the deprecation of the “majority of the
8 API surface”—namely, the APIs that were the most essential parts of the Facebook Platform.

9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED]

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

FILED UNDER SEAL**E. The Decision to Remove Developer Access to the Friends, News Feed, Events, and Other Crucial APIs Lacked Any Legitimate Justification**

181. The engineers tasked with implementing Zuckerberg’s decision to restrict access to the APIs were baffled. The decision made no technical sense whatsoever. Indeed, there was no justification for it other than to squelch competitors who threatened Facebook’s dominant position and DTBE.

182. As Facebook engineer, David Poll, had written to all Platform Engineers earlier in 2011, the decision would mean gutting the Facebook Platform of functionality used—and needed—by some of the most important mobile apps built on Facebook’s Platform:

I was thinking about the Platform 3.0 friend list change a bit as I was using my Android phone tonight and realized that two for the apps that most impact my day-to-day mobile experience will be completely, irrevocably broken by this change In both of these cases, the apps are adding real value to my experience, and in both of those cases, I have zero expectation that any of my friends will be using the app. The fundamental problem I’m having with this change is that my friend list is my information—it’s part of who I am, and for Facebook to shut down this access primarily comes across to me as FB intruding upon and shutting down my own access to my own information.

183. Poll concluded, “No matter how you slice it, this change is going to have a significant negative impact on my day-to-day smartphone experience.”

184. Poll was correct. The change meant breaking applications that added significant value to Facebook’s network and increased valuable user engagement on Facebook’s core product. The decision to deliberately break these applications had only one plausible purpose—to strengthen the DTBE and to ensure that competitors could not create rival social networks that could compete with Facebook.

185. That proposition was entirely obvious to those responsible for Facebook’s Platform. In an August 2013 e-mail, senior Platform engineer Bryan Klimt wrote to Ilya Sukhar, Facebook’s Head of Developer Products and Senior Engineer working on its APIs, and others working on Facebook’s Platform, stating that the reason for the decision to block access to the Friends and News Feed APIs was to exclude competitors and that all other reasons were simply false and pretextual. To begin with, Klimt was clear that the removal of the APIs was “ridiculous” because they were so essential to the Facebook Platform:

FILED UNDER SEAL

1 I'm trying to write a post about how bad an idea it would be to remove the
2 api that lets you get a list of user's friends from Facebook Platform. In order
3 to illustrate my point, I'd like to satirically suggest removing some API that
4 is so core to the developer experience and that removing it would be
5 ridiculous on its face. For example, removing the Windows API method
6 that lets you create a new window. Or removing the Twilio API method
7 that lets you send a text message. Both suggestions are utterly insane. The
8 problem is, for Facebook Platform, removing the method to let you get a
9 list of friends literally is already that ridiculous. I can't think of an example
10 more ridiculous to parody it with.

11 186. Klimt then dispelled any notion that the APIs were being removed for any technical or
12 functionality-driven reason:

13 Before we discuss in more detail, I'd like to clear up some misconceptions
14 about the deprecations. I've heard some rumors floating around about why
15 we are doing this. But many of them are clearly pabulum designed to make
16 engineers think this decision has solid technical reasons. It does not. 1/ This
17 API can be abused so we can remove it. False. That is a non-sequitur. Lots
18 of APIs can be abused. Our whole product can be abused. That's why we
19 have one of the best teams in the industry at detecting and stemming abuse.
20 That team, plus Unified Review, is more than sufficient to deal with any
21 theoretical abuse coming from this API. Even if this were true, who wants
22 to be in that classroom where the whole class is punished for transgressions
23 of a few?

24 187. Klimt also was clear that the APIs were not being removed in favor of new or different
25 APIs providing the same features:

26 2/ It's okay to remove because we've provided alternatives for common
27 uses. False. If you think that's true, then I don't think you realize why
28 developer platforms exist. If we wanted to limit Facebook to the set of use
cases we've already imagined, we could just do that ourselves, and not even
have a Platform. The purpose of a Platform is to let people build new things
on top of it. It's to enable the whole universe of ideas that anyone in the
world could think of. Developers out there will have all sorts of crazy ideas.
We want them to build those crazy ideas on top of Facebook. Do you know
why Facebook was originally built for the WWW instead of being part of
CompuServe or AOL's proprietary networks? It's because the web is an
open and extensible platform. It lets developers make their craziest become
reality.

188. Klimt then explained that the real reason was to hurt Facebook's competitors and prevent
them from competing with Facebook:

FILED UNDER SEAL

So, if neither of those reasons explains why we are doing this, what's driving it? The only reason I've heard that makes sense is that we are worried about people "stealing the graph", ***we are doing this as a protectionist grab to make sure no one else can make a competing social network by bootstrapping with our social graph.*** Okay, so let's assume for a minute that the social graph does belong to us, and not to our users. And let's even go so far as to assume that this is a real problem, although, I'm not convinced it is. I mean, concerns that other companies will steal our friend graph may just be paranoia. But for the sake of argument, let's say it's not. Then what? ***We're removing the core API in our developer platform. Out of concerns that someone will steal our social network product.*** That sends a clear message to developers: Facebook Platform comes second to Facebook the Social Network Product. This has been a criticism all along with our Platform. When you go read the blog posts critical of our Platform, they all hit on this same point. When our APIs are subjugated to the whims of our other products, they can't be stable. And an unstable platform isn't really a platform at all. So then you are left with 2 big problems. 1/ How do you convince external developers to build on a platform where the most basic core APIs may be removed at any time? I mean, the only big value we bring to the table right now is in distribution and discovery, and that's going to encourage developers to do only the most superficial integration with Facebook. Basically, they're going to do just enough to be able to use Neko ads. 2/ How do you convince internal developers to work on Platform knowing it's only ever going to play second fiddle to the rest of the company? I mean why should any of us work on a product that could be crippled at any time to benefit another team? If I worked on Platform, I would be seriously reconsidering my options if this API gets deprecated.

(emphasis added).

189. Klimt was clear—the decision to remove the APIs lacked any technical or business justification other than to prevent a competitor from creating a competing social network, eroding the DTBE protecting Facebook's business. Any proffered justification by anyone at Facebook to the contrary was entirely pretextual.

190. Moreover, the decision to remove the APIs permanently destroyed the value of Facebook's Platform. If developers could not trust Facebook to maintain the APIs as stable parts of its Platform, they would not risk writing apps for the Platform in the future. The decision meant scuttling Facebook's valuable Platform for the ability to prevent a rival social network from taking hold.

FILED UNDER SEAL

1 191. Sukhar responded to Klimt, noting that he agreed and that he “talks about this every single
2 meeting.” His pleas to Vernal, Purdy and Zuckerberg to reverse their decision fell on deaf ears. The
3 decision had been made and Klimt and Sukhar would have to implement it.

4 192. Facebook continued its audit of apps that relied on the APIs. Most of the Apps were
5 important to the Facebook ecosystem. Indeed, Facebook acknowledged they “are not spammy or crap,
6 but apps users like a lot.” Nonetheless, Facebook’s Papamiltiadis concluded that, among others, apps like
7 Sunrise, Yahoo, IFTT, Friendcaster, MyLife, Sync.me, YouTube, Contacts+, and Bitly “overlap with
8 Facebook products” and “could compromise our success in those areas.”

9 193. Facebook’s careful monitoring of competitive apps continued well into 2013, and given
10 its heavy reliance on data secretly collected by Onavo, Facebook purchased Onavo on October 14, 2013.
11 Facebook used that data to determine which apps competed with its social network and thus posed a threat
12 to the DTBE. It then targeted those companies for withdrawal of API access and coerced data reciprocity
13 agreements.

14 194. In October 2013, Facebook’s Purdy reported that Facebook was dividing apps into “three
15 buckets: existing competitors, possible future competitors, developers that we have alignment with on
16 business model.” Facebook’s Eddie O’Neil believed that the “separation between those categories doesn’t
17 feel clean” and that the overlap was problematic. As O’Neil observed, “apps can transition from aligned
18 to competitive and will ultimately make us sad that we leaked a bunch of data to them when they were
19 aligned.”

20 195. Sukhar objected to the entire exercise, noting that he had been speaking to many dozens
21 of developers “who will get totally fucked by this and it won’t even be for the right reason.” Sukhar
22 explained that his “engineers think *this plan is insane* and I’m not going to support an all hands [meeting]
23 to convince them otherwise.” (emphasis added).

24 196. As Sukhar noted, the decision to withdraw the Friends, News Feed, and Events APIs from
25 the Platform made no technical sense whatsoever, and Sukhar could not bring himself to tell his
26 engineers—who saw through the ruse—otherwise. It was obvious that Facebook was seeking to squelch
27 potential competition—namely, by preventing user growth and engagement for competitive apps. As one
28

FILED UNDER SEAL

Facebook engineer commented about the obvious purpose of the plan to remove the APIs: “I understand we want to make it hard for a developer to grow a new app.”

197. The review of apps continued and specific decisions with respect to certain highly sensitive competitors were escalated to Mark Zuckerberg. As one internal Facebook e-mail explained:

We maintain a small list of strategic competitors that Mark personally reviewed. Apps produced by the companies on the list are subject to a number of restrictions outlined below. Any usage beyond that specified is not permitted without Mark level signoff.

198. In December 2013, Klimt complained to Sukhar about the audit and categorization process:

So we are literally going to group apps into buckets based on how scared we are of them and give them different APIs? How do we ever hope to document this? Put a link at the top of the page that says “Going to be building a messenger app? Click here to filter out the APIs we won’t let you use!”

And what if an app adds a feature that moves them from 2 to 1. Shit just breaks? And messaging app can’t use Facebook login? So the message is, “if you’re going to compete with us at all, make sure you don’t integrate with us at all.”? I am just dumbfounded.

199. As Poll recognized in response to Klimt’s complaint, the changes to Facebook’s Platform were “more than complicated, it’s sort of unethical.” Klimt agreed with the assessment, noting that the API removal “feels unethical somehow It just makes me feel like a bad person.”

F. Facebook Prepares to Announce Removal of the APIs

200. Zuckerberg decided to announce the API removal under the cover of a major change to the Facebook Platform, codenamed PS12N, which would be announced at the next Facebook F8 Developer Conference. Facebook’s engineers were accordingly instructed in September 2013 to bury the changes to the API and announce them quietly along with the changes that would be announced at the conference.

201. In the run-up to its API withdrawal announcement, Facebook continued its audit of applications on its platform that were using the APIs. During that process Facebook continued to classify

FILED UNDER SEAL

1 potential competitors, including LinkedIn and AirBnB, as companies that would be denied access with
2 no whitelist exception.

3 202. Although Facebook knew that the APIs were going to be removed by the next F8
4 conference, it continued to tell developers to rely on them. As a Facebook Platform evangelist noted about
5 one particular document frequently shared with developers, “the language in here around friend
6 permissions is very counter to our upcoming platform simplification efforts” and “feels against the spirit
7 of where we are headed.”

8 203. That was, however, precisely what Facebook wanted—to continue to entice developers to
9 build their software and their businesses on APIs that made them dependent on Facebook. The use of the
10 APIs meant that competitors could be abruptly shut out of the market, useful apps could be extorted for
11 valuable social data, and the rest could simply be destroyed.

12 204. By October 2013, Facebook required certain application developers it chose to whitelist
13 to sign Private Extended API Agreements, which obligated them to purchase large amounts of advertising
14 or to provide their own valuable social data to Facebook in exchange for continued access. That month,
15 for example, Facebook whitelisted Royal Bank of Canada’s application in exchange for the purchase of
16 social data through Facebook’s NEKO advertising platform. [REDACTED]
17 [REDACTED]
18 [REDACTED]

19 205. Facebook catalogued and tracked developers on its platform that would likely complain
20 about the decision, creating negative press. Facebook’s internal employees tasked with crafting a PR
21 message explained the undertaking in a December 2013 e-mail:

22 In prep for Platform Simplification, we’re putting together a list of
23 developers who we think could be noisy and negative in press about the
24 changes we’re making: Primarily we think it will be a list of the usual
25 suspects from past policy enforcements. We’d love to pull from your
26 historic knowledge on the topic. Is there anybody you’d add to the list
27 below? We’re going to build plans around how we manage and
28 communicate with each of these developers. There are also comms plans
in the works for working with developers who are high ad spenders and
friends of Mark/Sheryl.”

FILED UNDER SEAL

206. Facebook planned to manage its message carefully, as its decision likely would alienate even those developers who were making large purchases of social data from Facebook through ads and/or who were friends of Facebook’s two most senior executives, Zuckerberg and Sandberg. Those developers were identified and the message to them was carefully crafted to avoid a PR disaster. For most application developers, however, the decision would result in the complete exclusion of their applications from Facebook’s ecosystem—which would likely be fatal to their businesses.

207. Facebook targeted potentially “noisy” or “negative” developers individually, including, but not limited to, the following applications and developers: iLike, Rock You, Zynga, Path, Flipboard, Slide, Social, Fixer, SocialCam, Viddy, BranchOut, Vince, Voxer, Message Me, Lulu, Anil Dash, Super Cell, Kabam, Washington Post, Guardian, The Wall Street Journal, Jason Calacanis, Cir.cl, Bang with Friends, Tinder, Social Roulette, App Wonder, Ark, Vintage Camera, and Girls Around Me.

208. Facebook also used call-log data secretly collected by Android users to target developers and applications to be shut down.

209. The entire process led Facebook engineer George Lee to lament:

We sold developers a bill of goods around implicit OG [Open Graph] 2 years ago and have been telling them ever since that one of the best things they could do is to a/b/ test and optimize the content and creative. Now that we have successes . . . We’re talking about taking it away . . . [Developers] have invested a lot of time to establish that traffic in our system . . . The more I think about this, the more concern I have over the pile of asks were [sic] making of our developers this year. PS12N is going to require them to alter how they deal with APIs (and for limited value).

210. Thus, as Facebook continued to prepare its API withdrawal announcement, Facebook’s own executives recognized that Platform developers had been conned into relying on Facebook’s APIs. Facebook knew full well that it intended to remove the APIs, but it allowed and encouraged developers to build entire businesses on and around them. As Lee put it, they were sold a “bill of goods.”

211. By 2014, it was clear that with the exception of a few apps and developers, most would be denied access entirely to the Friends, News Feed, and Events APIs.

FILED UNDER SEAL

1 212. In January 2014, Zuckerberg debated denying API access to dating apps. Facebook
2 decided that it would whitelist Tinder and other anointed dating apps and shut down the rest, clearing the
3 way for the selected apps to dominate the dating market. Zuckerberg reasoned that although Facebook
4 would ultimately create its own dating app, it would let Tinder and a select few others to survive until
5 Facebook's competing app was ready:

6 I've been thinking a lot about Tinder and other people recommendation
7 apps since about 10% of people in many countries are using a Tinder now.
8 People recommendations seems like something that should be right up our
9 alley, but it's currently something we're not very good at. Tinder's growth
10 is especially alarming to me because their product is built completely on
11 Facebook data, and it's much better than anything we've built for
recommendations using the same corpus I think this is a big and
important space and it's something we should have a team working on—
probably to develop people recommendation Hunch sections for now.

12 213. Zuckerberg became increasingly involved in assessing whether individual apps would be
13 whitelisted when the APIs were removed. Facebook's senior-most executives accordingly prepared
14 recommendations for his consideration. In a January 2014 presentation entitled, "Slides for Mark," for
15 example, Facebook employees summarized the results of the ongoing app audit. The presentation
16 observed that the changes would make it "impossible to build" an app without a whitelist agreement with
17 Facebook. The presentation made special recommendations for apps that purchased large amounts of
18 social data through Facebook's NEKO platform or whose developers were friends with Zuckerberg or
19 Sandberg. The bulk of the 41,191 apps that relied on the Friends, News Feed, or Events APIs, however,
20 would be shut out and, as a result, completely destroyed.

21 214. Although the effect on these apps was clear, Facebook continued to evangelize the APIs
22 to developers. In January 2014, Facebook's George Lee sounded the alarm to Purdy and Vernal, which
23 fell on willfully deaf ears:

24 [P]artner managers are still selling products that we ask them to sell, so
25 when it comes to feed integration, we're still telling people to use [Open
26 Graph]. The last f8 was all about implicit [Open Graph], so while we may
27 have decided amongst ourselves that this is no longer the future without an
28 alternative we don't have anything to tell current [developers] (so partners

FILED UNDER SEAL

1 continue to tell them to use [Open Graph] and they continue to integrate
2 it).

3 215. The plan to quietly take away the APIs in favor of a new crippled developer platform was
4 called the “switcharoo plan” by Facebook’s engineers. It was clear to all involved that the announcement
5 of the changes to the platform at the upcoming F8 conference was cover for the radical changes Facebook
6 planned to make to its platform—namely, the removal of the Friends, News Feed, and Events APIs.

7 216. During March 2014, Facebook’s engineers and employees continued to be baffled by the
8 upcoming decision. As one employee noted:

9 It seems a bit odd that we block other developers from doing things on our
10 platform that we’re ok with doing ourselves. Do we consider ourselves
11 exempted? That seems a little unfair especially when our stance on some
12 of these policies is that they’re about ensuring trusts and a great experience.
13 My mental model on how platform is a level playing field could be way off
14 though.

15 217. The decision made no sense to Facebook’s own employees, particularly because Facebook
16 itself needed the APIs to make their own competing applications, including Facebook’s Messenger
17 application. Facebook’s executives ignored all of the concerns raised by their employees, including their
18 API engineers, and continued to drive towards the announcement of the removal of the APIs at F8.

19 218. The real reason for the removal of the APIs was kept tightly under wraps. In April 2014,
20 right before the announcement, Vernal warned Sukhar that if any mention was made of the competitive
21 reasons for the removal of the APIs (as Sukhar wanted), there would be a “high likelihood of breaking
22 into jail.”

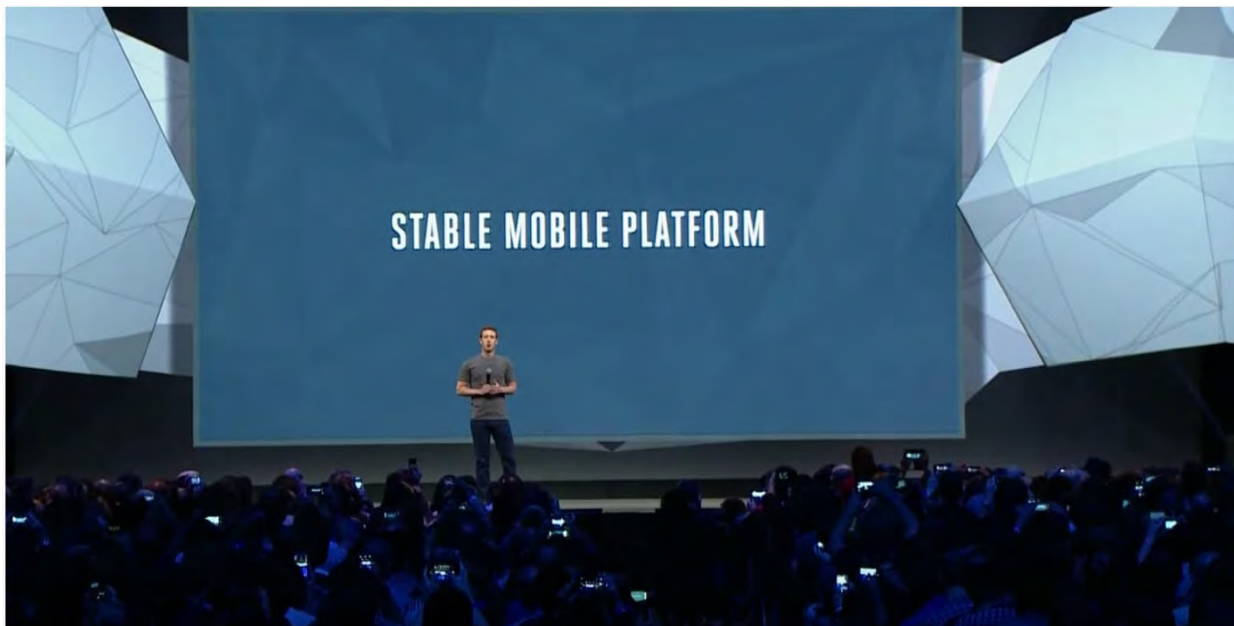
23 **G. The Announcement at F8**

24 219. On April 30, 2014, Facebook announced “The New Facebook Login and Graph API 2.0”
25 on Facebook’s website. Facebook heralded changes to its new Login system for several pages. Buried in
26 the announcement was a quiet statement about the Platform’s most important APIs—the Friend, News
27 Feed, and Events APIs: “In addition to the above, we are removing several rarely used API endpoints;
28 visit our changelog for details.”

FILED UNDER SEAL

220. These APIs were not *rarely used* at all. Tens of thousands of third-party apps were actively using and building on the APIs. Internal Facebook engineers likened them to essential APIs in Microsoft's Windows and were outraged at the removal. Five of the top ten Facebook Apps surveyed in December 2012 relied heavily on them. The announcement was entirely false and was deliberately buried beneath other API announcements to avoid drawing attention to the competition-crippling effect of the decision. In fact, today, the changelog referred to in the announcement is no longer accessible on Facebook's page even though years of other changes are.

221. When Mark Zuckerberg took the stage at F8 days later for his keynote speech, there was no mention of the removed APIs. Instead, Zuckerberg emphasized the "stability" of Facebook's mobile platform just as Facebook quietly removed some of the most heavily relied-upon and necessary APIs in Facebook's Platform.



222. At the twenty developer sessions preceding the announcement, not one mention was made of the API removal or that the upcoming changes would simply break nearly all of the more than 40,000 third-party apps that relied on the APIs.

IV. THE SURVEILLANCE AND ACQUISITION OF COMPETITIVE THREATS

223. To ensure that its scheme to maintain and expand its market power would work, Facebook had to control an important source of competition: independent social networks and producers of social

FILED UNDER SEAL

1 data. Although Facebook could simply destroy any competition that relied on its Platform by denying
 2 access to essential APIs, this would do nothing to stop a competitor that was growing its network of
 3 engaged users entirely independent of Facebook.

4 224. To detect such threats before they became too formidable, Facebook sought a way to
 5 covertly surveil millions of mobile users to determine what applications they were using, and how. Mobile
 6 applications were particularly important—and concerning—to Facebook, as desktop engagement was
 7 shrinking while mobile apps rapidly proliferated. By 2012, it was clear to Zuckerberg and to Facebook
 8 that any threat to its dominance would come from a mobile application. As explained in this section,
 9 Facebook used mobile spyware on an unprecedented scale to surveil, identify, and eventually remove
 10 from the market through acquisition competitors that independently threatened Facebook’s dominance
 11 and/or the DTBE protecting its monopoly, market power and business.

12 **A. Facebook Relies on Onavo’s Surveillance of Facebook’s Competitors, and**
 13 **Acquires and Uses Onavo’s Assets**

14 225. Onavo was an Israeli mobile web analytics company founded by Roi Tiger and Guy Rosen
 15 in 2010. The company designed spyware designed to surveil users as they used their mobile devices. To
 16 obtain extensive information on a user’s usage of mobile applications and of bandwidth, Onavo cloaked
 17 its spyware in virtual private networks (“VPNs”), data compression, and even in mobile privacy apps.

18 226. Onavo sold the mobile usage data it collected to Facebook, which in turn used the real-
 19 time information it received from Onavo to determine which mobile applications posed a threat to
 20 Facebook’s dominance and to the DTBE protecting Facebook from new entrants and competition.
 21 Facebook used Onavo data to: (a) identify and target competitors from which Facebook could demand
 22 Whitelist and Data Sharing Agreements; (b) identify and target competitors to whom Facebook would
 23 completely deny Platform access; and (c) identify and target competitors that Facebook would remove
 24 from the competitive landscape entirely through acquisition.

25 227. Facebook received Onavo information in real time, which included the two most important
 26 metrics for competing mobile applications—their reach and engagement. Reach measures the size of an
 27 application’s user base, and “engagement” measures the extent to which users actively engage with the
 28

FILED UNDER SEAL

1 application. An application with high reach but low engagement cannot generate the sort of social data
2 that Facebook needs to feed its advertising platform with actionable targeting data. Conversely, an
3 application with high engagement but low reach doesn't generate social data from enough people to
4 attract a broad base of advertisers. The greatest threat to Facebook's business would come from an
5 application that exhibited strong reach and strong engagement—and especially one that showed rapid
6 growth in both metrics, indicating the development of network effects.

7 228. As the potential threat to its market dominance from mobile applications continued to
8 grow, Facebook sought to obtain exclusive control over Onavo's surveillance data—and over its mobile
9 spyware code and installed base. On October 13, 2013, Facebook acquired Onavo.

10 229. On its blog, Onavo's CEO Guy Rosen and CTO Roi Tiger, announced that Onavo would
11 continue as a standalone brand: "When the transaction closes, we plan to continue running the Onavo
12 mobile utility apps as a standalone brand. As always, we remain committed to the privacy of people who
13 use our application, and that commitment will not change."

14 230. Facebook, however, had other plans. It immediately began integrating Onavo's
15 applications into both its business operations and its acquisition strategy. Facebook, for example, began
16 analyzing data secretly collected from Onavo's Protect software, which was a massive surveillance and
17 data collection scheme disguised as VPN software. Billed as a way to "keep you and your data safe,"
18 Onavo Protect in fact monitored all web and mobile application traffic on a user's mobile device.

19 231. When an Onavo Protect user opened a mobile app or website, Onavo software secretly
20 redirected the traffic to Facebook's servers, where the action was logged in a massive database. Facebook
21 product teams then analyzed the aggregated Onavo data to determine which apps and features people
22 were using in real time, how frequently they used the apps, and for how long. If the data in an app was
23 not encrypted, this information was as specific as (for example) the number of photos the average user
24 likes or posts in a week in that app.

25 232. Based on a 2017 estimate, Onavo's mobile apps were downloaded an estimated twenty-
26 four million times, and Facebook collected, compiled, and leveraged all of the collected data. By February
27 2018, Onavo apps had been downloaded thirty-three million times across both iOS and Android.

FILED UNDER SEAL

233. As the former chief technologist for the Federal Trade Commission remarked to the press, Onavo was being leveraged against user interests to stifle competitive innovation:

Instead of converting data for the purpose of advertising, they're converting it to competitive intelligence Essentially this approach takes data generated by consumers and uses it in ways that directly hurts their interests—for example, to impede competitive innovation.

234. Since 2011 and through the present, Onavo products have provided Facebook with real time data about mobile users on a breadth and scale not available through any other service or app. Using Onavo data, Facebook was able to determine which potential competitors it could target for its Whitelist and Data Sharing agreements; which competitors it could destroy by denying access to crucial APIs; and which competitors is needed to remove from the market through acquisition to preserve its monopoly position and DTBE.

235. Moreover, by monitoring potential threats, Facebook ensured that it had no blind spot—any application that posed a threat to its dominance was dealt with through anticompetitive and unlawful Whitelist and Data Sharing Agreements, destruction by denial of access to vital APIs on Facebook's platform, or by acquisition.

236. By acquiring Onavo, Facebook obtained exclusive access to the only real-time and high-quality source for mobile app user metrics at scale. Because of the acquisition of Onavo, Facebook strengthened the DTBE by ensuring that any threat to its dominance of the Social Advertising Market was dealt with at the earliest possible stage. Indeed, through Onavo, Facebook was able to (and did) track mobile app usage and trends essentially from launch. If a potential Facebook killer was on the rise, Facebook had a unique tool to identify it before anyone else could—and Facebook used it.

237. In the years after it acquired Onavo, Facebook continued to aggressively leverage the company's codebase in deceptively labeled apps that facilitated maximum surveillance and data collection of mobile users. For example, Facebook placed Onavo spyware in apps whose stated purposes required privileged access to user's mobile devices (in some cases, super-user privileges), allowing Facebook to gather data on virtually every aspect of a user's mobile device usage.

FILED UNDER SEAL

238. The abuses by Facebook were so flagrant that on August 22, 2018, Apple banned Facebook's Onavo app from its App Store. Apple ejected Facebook's app from its marketplace because it violated Apple's rules prohibiting apps from using data in ways far beyond what is required to run the app and provide advertising. In other words, because Onavo Protect was leveraging far more data than any VPN could conceivably need, it was clear that the true purpose of the app was to spy on Onavo users, and Apple would not allow it.

239. Indeed, the amount of surveillance was jaw-dropping. Facebook's Onavo Protect app reported on users' activities whether their screens were on or off; whether they used WiFi or cellular data; and even when the VPN was turned off. There was simply no rational relationship between the data collected and the purported purpose of the application. Put simply, a VPN that collected data even when the VPN was off was an obvious subterfuge for blatant spying on user behavior.

240. Undeterred, Facebook repackaged its Onavo spyware as a Facebook Research VPN app. Facebook sidestepped the App Store by rewarding teenagers and adults when they downloaded the Research app and gave it root—superuser—access to network traffic on their mobile devices. Facebook has been leveraging its Onavo code in similar ways since at least 2016, administering the program under the codename "Project Atlas"—a name suited to its goal of surveilling app usage on mobile devices in real time.

241. When the news broke in January 2019 that Facebook's Research apps were repackaged Onavo apps designed to spy on users, Facebook immediately withdrew the programs from the Apple App store.

242. Apple again concluded that Facebook had tried to violate its policies. Using Apple's Enterprise Developer Program, which allows the installation of a certificate or policy that provides root access to an iPhone or iPad, Facebook obtained a level of administrative privilege designed for a company's internal IT department. Thus, using a system that allowed organizations to manage their internal mobile devices, Facebook provided its spyware super user access to regular people's iPhones and iPads. Apple balked at the abuse. An Apple spokesman stated:

FILED UNDER SEAL

We designed our Enterprise Developer Program solely for the internal distribution of apps within an organization. Facebook has been using their membership to distribute a data-collecting app to customers, which is a clear breach of their agreement with Apple. Any developer using their enterprise certificates to distribute apps to consumers will have their certificates revoked, which is what we did in this case to protect our users and their data.

243. U.S. Senator Mark Warner immediately called for new legislation to prevent the sort of abuse which Facebook had engaged in. U.S. Senator Richard Blumenthal issued a fierce statement rebuking Facebook’s repackaging of the Onavo spyware app as “research”: “Wiretapping teens is not research, and it should never be permissible.”

244. In addition to Onavo’s Protect app, Facebook has attempted to deploy its surveillance software as other forms of utility applications that require extensive or privileged access to mobile devices. For example, Facebook released the Onavo Bolt app, which locked apps behind a passcode or fingerprint while it covertly surveilled users—and sent Facebook the results. Facebook also shut that app down the very day that its surveillance functionality was discovered. The Onavo Bolt app had been installed approximately 10 million times.

245. Facebook continues to possess Onavo’s code base and is likely, as it has done before, to repackage its surveillance software into yet another app. Facebook can also easily incorporate surveillance code into any of its mobile applications that enjoy massive installed bases and reach, including Instagram and WhatsApp. If left undeterred, Facebook will likely continue leveraging the surveillance software, infrastructure, and analysis that it acquired as part of its acquisition of Onavo.

B. Facebook Identifies Instagram as a Threat and Acquires the Company

246. Data from Onavo reported a significant threat on the horizon likely as early as 2011 (and certainly by 2012): a photo-sharing mobile application called Instagram. That app had its origins when founder Kevin Systrom, then 27, learned to code over nights and weekends. Systrom developed an app called Burbn, which allowed users to check in, post plans and share photos. The photo sharing feature immediately became the app’s most popular.

FILED UNDER SEAL

247. After meeting venture capitalists from Baseline Ventures and Andreessen Horowitz, Systrom received \$500,000 of funding. Systrom soon after met co-founder Mike Krieger—then 25 years old—who focused on the user experience of the app.

248. Seeing the positive reception to the photo sharing aspect of the Burbn app, Krieger and Systrom decided to pivot their business to focus on that feature. They studied their rivals in the category, including an app called Hipstamatic, which included photo-editing features, including the ability to add filters to photos. Hipstamatic, however, had no social capabilities.

249. Seeking to bridge the gap between Hipstamatic photo features and Facebook’s elements, Systrom and Krieger stripped Burbn down to its photo, comment, and like capabilities. They then renamed the app Instagram, containing the words “instant” and “telegram.”

250. Systrom and Krieger worked tirelessly to polish the user experience of their new application, designing Instagram to streamline the process of taking photos on mobile devices and uploading them to a social platform. The app had a minimalist focus, requiring as few actions as possible from the user. After eight weeks of fine-tuning, the app entered its beta phase and the founders prepared to launch it on iOS.

251. On October 6, 2010, Instagram launched on iOS. That very day it became the top free photo-sharing app on Apple’s App Store, racking up twenty-five thousand downloads. Instagram’s founders were stunned at the response. As Systrom noted after the launch: “First off, we have to say that we never expected the overwhelming response that we’ve seen. We went from literally a handful of users to the #1 free photography app in a matter of hours.”

252. By the end of the first week, Instagram had been downloaded 100,000 times, and by mid-December 2010, its total downloads had reached one million. The timing of the app was impeccable, as the iPhone 4, with its improved camera, had launched just a few months earlier in June 2010.

253. With Instagram on the rise, investors clamored for a stake. In February 2011, Instagram raised \$7 million in Series A funding from a variety of investors, including Benchmark Capital, which valued the company at around \$25 million. In March 2011, Jack Dorsey, the CEO of Twitter, pursued the

FILED UNDER SEAL

1 idea of acquiring Instagram, and Twitter made an offer of approximately \$500 million dollars for the
2 company. Systrom declined.

3 254. By March 2012, the app's user base had swelled to 27 million. That April, Instagram was
4 released on Android phones and was downloaded more than one million times in less than one day. At
5 the time, the company was also in talks to receive another \$500 million funding round.

6 255. Internally, Facebook carefully tracked Instagram's meteoric rise, including through the
7 intelligence it received from Onavo's data collection. Instagram clearly posed a competitive threat to
8 Facebook's dominant position, including in the rapidly expanding market for mobile-based social
9 applications.

10 256. Unlike Instagram's streamlined approach to photo sharing, Facebook's photo-sharing was
11 onerous. As Facebook internally recognized, mobile devices were changing how users uploaded and
12 shared photos and it was causing severe problems for Facebook's business. As an internal Facebook
13 presentation explained:

14 Before phones, people would take their digital cameras out for special
15 events, vacations, etc. Then, they would post a bunch of photos at once—
16 after uploading them to their computer. With phones, people take and share
17 more photos more often. They share them individually (rather than waiting
18 to upload a bunch at once).

19 257. This resulted in a large drop in bulk photo uploads on Facebook's core social networking
20 product—a 29% decline from 2012 to 2014. Facebook also observed that text posts were “tanking” 26%
21 because of “migration to phones with cameras.” The data was clear—Facebook had to shut down the
22 looming threat from the new photo-sharing app. If Facebook did nothing, Instagram's user base would
23 imminently eclipse Facebook's at its current growth rate, eroding and perhaps even destroying
24 Facebook's DTBE. An independent app with no ties or reliance on Facebook, Instagram could become
25 not only a competing mobile-based social app, but a social network unto itself that could rival Facebook
26 in the amount of engagement and social data it could produce and monetize.

27 258. In February 2012, Zuckerberg discussed the potential acquisition of Instagram with
28 Facebook Chief Financial Officer, David Ebersman. Zuckerberg explained that he had “been thinking

FILED UNDER SEAL

1 about . . . how much [Facebook] should be willing to pay to acquire mobile app companies like
2 Instagram . . . that are building networks that are competitive with our own.” Mr. Zuckerberg told Mr.
3 Ebersman that these “businesses are nascent but the networks are established, the brands are already
4 meaningful and if they grow to a large scale they could be very disruptive to us.”

5 259. In response, Ebersman asked Zuckerberg whether the goals of the acquisition would be
6 to: (1) neutralize a potential competitor; (2) acquire talent; or (3) integrate Instagram’s product with
7 Facebook’s to improve its service. Zuckerberg replied that the purpose of the transaction would be to
8 neutralize Instagram, saying that the goals of the deal were “a combination of (1) and (3).” He explained:

9 One thing that may make (1) more reasonable here is that there are network
10 effects around social products and a finite number of different social
11 mechanics to invent. Once someone wins at a specific mechanic, it’s
12 difficult for others to supplant them without doing something different. It’s
13 possible someone beats Instagram by building something that is better to
the point that they get network migration, but this is harder as long as
Instagram keeps running as a product.

14 260. Zuckerberg quickly understood that Instagram’s meteoric rise was a threat to Facebook’s
entire business. With a ready-made network of users, Instagram’s dominance of one of the “mechanics”
15 fueling Facebook’s engagement would mean the disruption of the DTBE protecting Facebook. If
16 Instagram took away engagement from Facebook, Facebook would lose some of its ability to target users
17 for content and to advertise to them, which in turn meant less engagement. The virtuous circle would
18 reverse itself.

19 261. As Zuckerberg himself put it:

20 By a combination of (1) and (3), one way of looking at this is that what
21 we’re really buying is time. Even if some new competitor springs [sic] up,
22 buying Instagram, Path, Foursquare, etc [sic] now will give us a year or
23 more to integrate their dynamics before anyone can get close to their scale
again. Within that time, if we incorporate the social mechanics they were
24 using, those new products won’t get much traction since we’ll already have
their mechanics deployed at scale.

25 262. It was clear to Zuckerberg that what he was “really buying is time,” as eventually a
26 competitor would emerge that threatened Facebook’s DTBE and dominance over its walled garden.

FILED UNDER SEAL

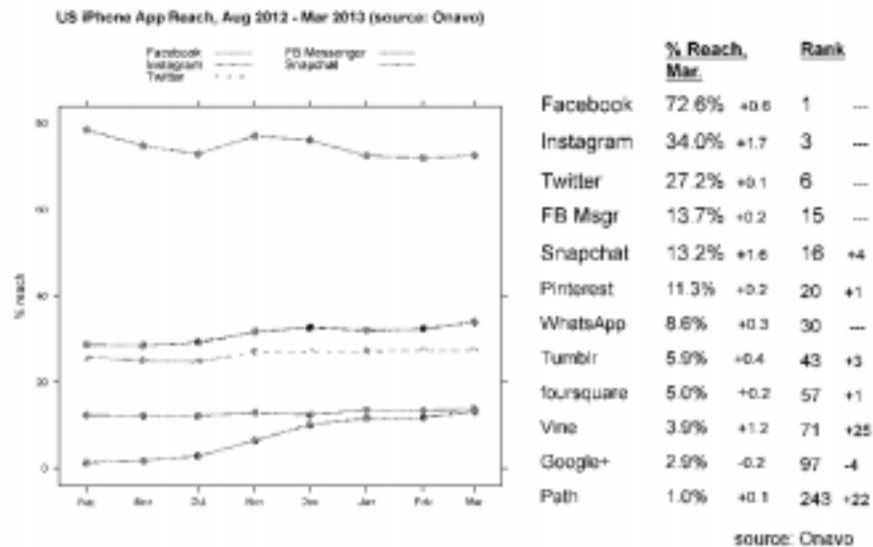
1 Zuckerberg continued the discussion through March 2012, telling Mike Schroepfer, Facebook’s Chief
2 Technology Officer, that acquiring Instagram would provide the company with “[i]nsurance” for
3 Facebook’s main product. Schroepfer agreed, responding that “not losing strategic position in photos is
4 worth a lot of money.” He added that the “biggest risk” would be if Facebook were to “kill” Instagram
5 “by not investing in the company and thereby opening a window for a new entrant.”

6 263. In a message to another Facebook employee on April 5, 2012, Zuckerberg said that
7 “Instagram can hurt us meaningfully without becoming a huge business.” In contrast, he did not view
8 other smaller firms, such as Pinterest and Foursquare, as imminently dangerous competitive threats. As
9 he noted, if these companies “become big we’ll just regret not doing them . . . Or we can buy them then,
10 or build them along the way.” In an all-hands meeting the following day, Mr. Zuckerberg responded to a
11 question about Instagram’s rapid growth by saying that “we need to dig ourselves out of a hole.” He also
12 told employees at the company that Instagram is “growing really quickly” and that it would be “tough to
13 dislodge them.”

14 264. After direct talks with Mark Zuckerberg, Facebook made Instagram an offer to purchase
15 the company for \$1 billion in April 2012, with the express promise that the company would remain
16 independently managed. Facebook consummated the deal immediately prior to its IPO.

FILED UNDER SEAL

265. Facebook's own Onavo data, which was obtained and published by BuzzFeed, made clear that Instagram posed an existential threat to Facebook. By February 2013, Instagram had grown to 34% of the total user reach among all social apps.

US mobile apps (iPhone)

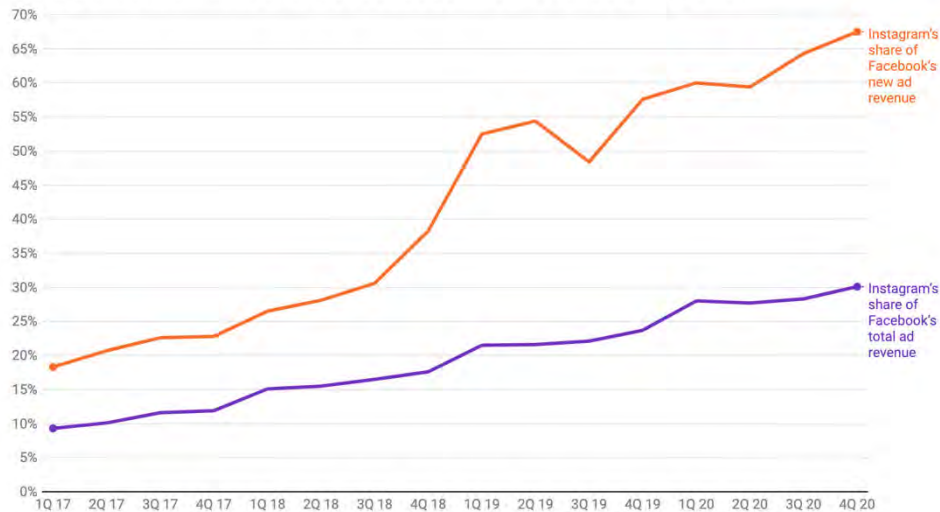
266. With its Instagram acquisition, Facebook's share of mobile photo sharing app users ballooned as Facebook added Instagram's 34% user reach to Facebook's own 72% user reach.

267. Although Instagram had not at the time of the merger meaningfully monetized its user engagement and social data, Facebook quickly did so. By the end of 2013, Facebook had begun showing ads on Instagram. Since then, Instagram has become an ever-increasing proportion of Facebook's advertising revenue and a large share of Facebook's user growth.

FILED UNDER SEAL

268. In 2017, Instagram generated \$2 billion, or about 15 percent, of Facebook's \$13 billion in ad revenue.

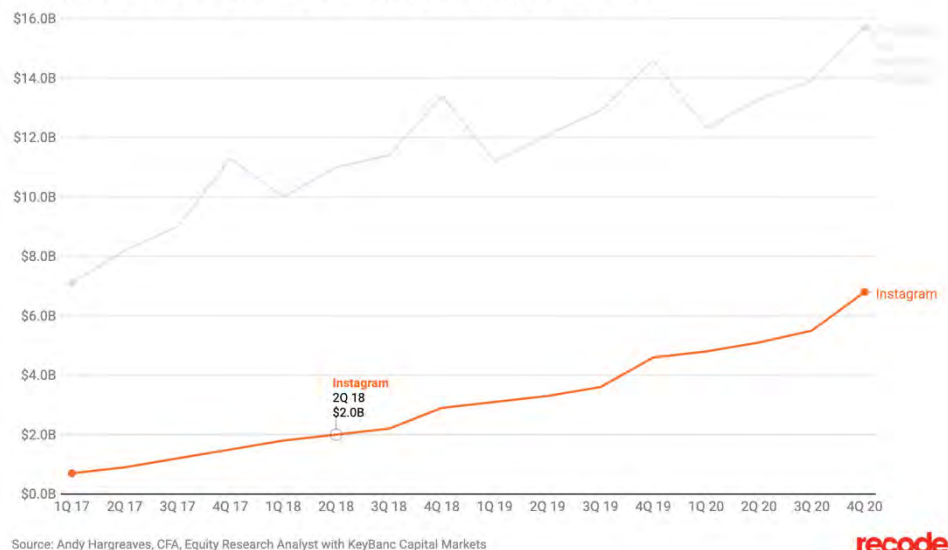
Instagram's estimated share of Facebook's ad revenue and growth



269. By the end of 2018, Instagram had a billion users and was estimated to generate \$8 billion to \$9 billion in revenue for Facebook in 2018.

270. Instagram also accounts for the bulk of Facebook's new revenue since the acquisition.

Facebook and Instagram's estimated quarterly ad revenue



FILED UNDER SEAL

271. Instagram allowed Facebook to grow its social network as Facebook’s desktop and core mobile application began to stagnate. Together, Facebook and Instagram captured and monetized the social data generated across both apps.

272. The Instagram acquisition ensured that Instagram could not become a rival social network that could generate enough social data to erode the DTBE protecting Facebook’s business. It also ensured that Instagram could not build and grow its own developer platform, which would threaten Facebook’s scheme to dominate the Social Advertising Market by denying and/or leveraging social-data dependent applications’ access to essential functionality. The acquisition accordingly also ensured that Facebook rivals required to enter into Whitelist and Data Sharing Agreements had no other platform choice—and thus no option but to hand over their social data to Facebook. Finally, the acquisition ensured that Instagram could not sell highly targeted advertising in the Social Advertising Market, which would mean there would be a material check on Facebook’s ability to raise prices.

273. At the time of its IPO in 2012, Facebook struggled to grow its mobile product, let alone to meaningfully monetize the social data it collected through advertising. By 2019, Facebook had achieved an 83% share of the Social Advertising Market by leveraging its Instagram mobile application and its Facebook mobile and desktop applications. No other company comes close in market share.

274. Instagram was instrumental to Facebook’s explosive growth in the Social Advertising Market. From the fourth quarter of 2010 until the first quarter of 2011, Facebook’s revenue was flat. From 2011’s holiday cycle to 2012’s opening three months (right before its IPO), Facebook actually *shrank*. Facebook then experienced a sudden reversal after its acquisition of Instagram, as mobile revenue began to account for a significant share of revenues, and Instagram allowed Facebook to grow with the rise of mobile applications.

275. Notably, Facebook’s acquisition of Instagram also allowed Facebook to exclude third-party apps that provided photo and video sharing functionality from its Platform. If an image sharing or video app contained an important feature, Facebook cloned it, thus paving the way for excluding a competitive rival from its Platform, while simultaneously taking away that rival’s share of users.

FILED UNDER SEAL

276. For example, when Snap, the maker of the app SnapChat, rejected Zuckerberg and Facebook’s \$3 billion offer to purchase the company and its product, Facebook flagrantly copied key features from Snap and built it into its Instagram product. Thus, when the SnapChat’s “stories” feature—which allows a user to post a connected series of images and video—rapidly grew in popularity, Instagram simply cloned it. By late 2016, Instagram had launched a product that mooted one of Snapchat’s most popular features.

277. Facebook’s own clunky mobile app’s clone of the “stories” feature did not have nearly the same traction with users. It was Instagram that provided Facebook the platform to compete head-on with a looming threat among social photo- and video-sharing apps. Without Instagram, Facebook would have faced direct competition. Instead, it leveraged Instagram to obtain and maintain its dominance among social mobile apps and the lucrative social data they generated.

278. Put simply, the acquisition of Instagram dramatically increased Facebook’s market share of the Social Advertising Market and strengthened the DTBE protecting Facebook’s business.

C. Facebook Acquires WhatsApp

279. In February 2009, Jan Koum and Brian Acton left Yahoo and founded a new company called WhatsApp. Koum had an idea for a mobile application that displayed user statuses in an address book on a smartphone—indicating, for example, whether a user was on a call, had low battery, or was at the gym. The pair enlisted the help of a Russian developer, Igor Solomennikov, to build the app. Koum spent days writing backend code for the app to allow it to sync with any phone number in the world.

280. Although the app—named WhatsApp—was initially unsuccessful, a June 2009 development changed everything. That month, Apple introduced “push notifications” for iPhone, allowing developers to ping app users even when they weren’t using the app. Koum immediately updated WhatsApp to ping a user’s entire network of friends when their status changed.

281. The feature eventually became a form of instant messaging. Because messages sent through WhatsApp instantaneously notified other users even if the phone was not running the app in the foreground, it became ideal for broadcasting messages to connections within a user’s social network, which was built on their phone’s contact list.

FILED UNDER SEAL

1 282. At the time, WhatsApp's only significant competition for this sort of instant messaging
2 was BlackBerry's BBM—which was exclusive to BlackBerry's proprietary hardware platform.
3 WhatsApp, on the other hand, tapped into the vast network of app-enabled consumer smartphones that
4 had emerged, particularly Apple's iPhone.

5 283. WhatsApp continued to innovate, including by introducing a double checkmark that
6 showed when a message was read by another user. Wanting more from text messaging, including the
7 limited MMS protocol used by cellular networks, WhatsApp set out to build a multimedia messenger
8 system to send messages across a social network in real time to mobile devices.

9 284. Because WhatsApp's messaging used the mobile phone's Internet connection rather than
10 text messages, the app allowed users to avoid text messaging fees entirely. In some countries, text
11 messages through cellular providers were metered. WhatsApp's ability to send messages to any user with
12 a phone using the Internet was its most sought-after feature.

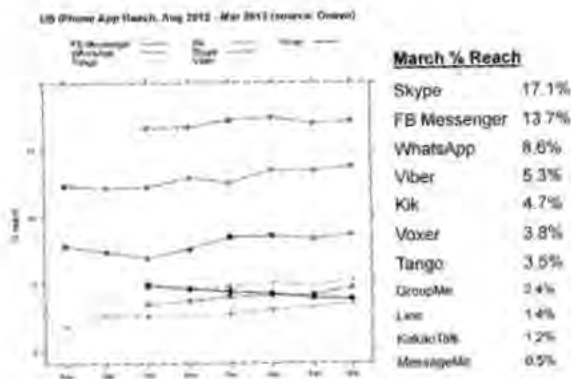
13 285. In December 2009, WhatsApp updated its app for the iPhone to send photos. User growth
14 spiked, even when WhatsApp charged users for its service. Having created a unique combination of image
15 and messaging apps as one socially powered app, WhatsApp decided to stay a paid service and grew
16 while generating revenue.

17 286. By early 2011, WhatsApp was one of the top twenty paid apps in Apple's U.S. App Store.
18 The company attracted the attention of venture capital firm Sequoia, and WhatsApp agreed to take \$8
19 million of additional funding in addition to its original \$250,000 seed funding.

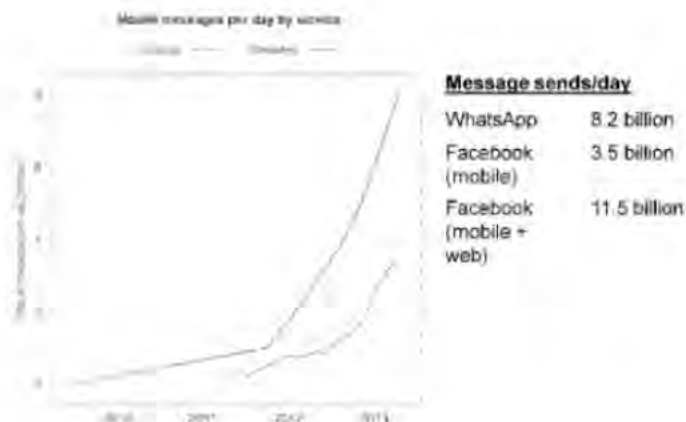
20 287. Two years later, in February 2013, WhatsApp's user base had ballooned to 200 million
21 active users. That month, WhatsApp raised additional funds—another \$50 million from Sequoia, at a
22 valuation of \$1.5 billion.

FILED UNDER SEAL

288. Internally, Facebook had carefully tracked WhatsApp's rapid rise. Engagement data from Facebook's Onavo spyware reported that WhatsApp was rivaling Facebook's own Messenger product and held third place in terms of user reach among mobile messenger apps for iPhone in the U.S. as of April 2013.

US mobile messenger apps (iPhone)

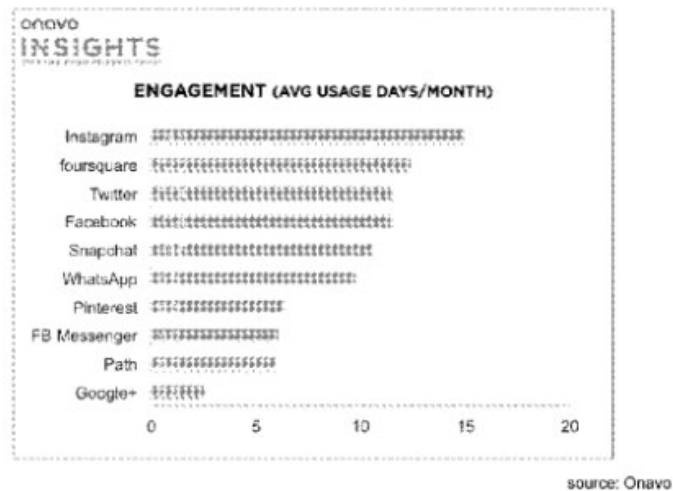
289. The broader picture was even more threatening to Facebook. As BuzzFeed reported, Onavo had tracked messages sent through WhatsApp and the number dwarfed Facebook's own mobile product by more than twofold.

WhatsApp message sends

FILED UNDER SEAL

290. The same Onavo data reported by BuzzFeed showed massive engagement among WhatsApp users, placing it in sixth place behind Facebook's own core product; Facebook's newly acquired Instagram; Twitter; Foursquare; and Snapchat.

US mobile apps (iPhone only)



291. WhatsApp, although lacking Facebook's market reach, was drawing from the same pool of limited attention. Given Facebook's own fledgling Messenger App, WhatsApp exposed a massive vulnerability in Facebook's business model. WhatsApp was built on a social network derived directly from a smartphone user's contact list. It did not require Facebook's graph network for growth and could not therefore be shut down by revoking access to Facebook's APIs. Nor could Facebook demand that WhatsApp enter into a Whitelist and Data Sharing agreement.

292. WhatsApp posed a direct threat to Facebook's business, including the DTBE protecting its dominance. WhatsApp allowed for statuses, image sharing, and texting—all of the principal features of Facebook's core products. By 2013, the size of WhatsApp's network and the user engagement in that network made WhatsApp the most direct threat to Facebook's market dominance—and because of Onavo, Facebook knew it.

293. To ensure that it maintained its DTBE, and thereby its dominance of the Social Advertising Market, Facebook sought to remove WhatsApp as a competitor. As the *Wall Street Journal* reported, Facebook's Vernal internally commented in 2013: "Whats App launching a competing platform is

FILED UNDER SEAL

1 definitely something I’m super-paranoid about.” Vernal understood that if WhatsApp created a rival
2 platform, Facebook’s own scheme to exclude rivals by leveraging its Platform would fail—developers
3 would migrate to the competing platform provided by WhatsApp.

4 294. Internally, Facebook’s management team discussed the WhatsApp threat with urgency.
5 Facebook Director of Growth Javier Olivan wrote in an internal e-mail that WhatsApp had higher levels
6 of reach and usage than Facebook in countries that it had penetrated. For example, based on Facebook’s
7 internal data, WhatsApp reached 99.9% of the smartphone population in Spain, or as Mr. Olivan
8 described it, “literally everyone.” By purchasing WhatsApp, Olivan suggested that they could “grow
9 Facebook even further” by exposing new users to Facebook. Additionally, by bundling free services with
10 WhatsApp and Facebook’s other services, the transaction could serve as another mechanism to expand
11 Facebook’s reach among WhatsApp users. Zuckerberg responded, “I really agree with this analysis.”

12 295. In an email to Facebook’s CFO, David Ebersman, Olivan wrote that WhatsApp’s “reach
13 amongst smartphone users is actually bigger than ours . . . we have close to 100% overlap, our user-base
14 being a subset of theirs.” He explained that “in markets where they do well, they literally reach 100% of
15 smartphone users—which is a big part of the population.”

16 296. On December 13, 2013, Zuckerberg wrote to his management on competitive issues facing
17 the company. WhatsApp was among them:

18 I want to call out two competitive near term issues we face. The first is
19 WhatsApp adding a feature like this for public figures . . . If the space is
20 going to move this direction, being the leader and establishing the brand
21 and network effects matters a lot. This alone should encourage us to
22 consider this soon. . . . When the world shifts like this, being first is how
23 you build a brand and network. We have an opportunity to do this at scale,
24 but that opportunity won’t last forever. I doubt we even have a year before
25 WhatsApp starts moving in this direction.

26 297. Using Onavo data, Facebook’s data scientists modeled WhatsApp’s growth, particularly
27 its engagement and reach, to determine whether it was “killing Facebook messenger,” as well as how its
28 usage trends compared to Snapchat.

FILED UNDER SEAL

298. Knowing about WhatsApp's size, its engagement, and its unique potential to erode the DTBE protecting Facebook market dominance, Facebook moved aggressively to remove this existential threat from the competitive landscape. In late 2013, Facebook made an initial bid of \$16 billion in stock for WhatsApp. During negotiations in early 2014, Facebook raised its price to \$19.6 billion—adding \$3.6 billion to the original price as compensation to WhatsApp employees for staying on board at Facebook. When all was said and done, Facebook ultimately paid close to \$22 billion for WhatsApp.

299. But for the value of containing and shutting down the growth of WhatsApp's competing social network and platform, the transaction made no possible economic sense to Facebook. WhatsApp's revenues were a meager \$10.2 million in 2013. Its six-month revenue for the first half of 2014 totaled \$15.9 million, and the company had incurred a staggering net loss of \$232 million in that same period. Facebook had paid twenty billion dollars—thousands of times WhatsApp's revenues—to acquire a money-losing company that created software functionality Facebook itself already had as part of its own products, and could easily build from scratch for a fraction of the cost of the acquisition if it wanted to.

300. At the time of the WhatsApp acquisition, Facebook's user reach and user base and engagement was already massive—and unrivaled by any competing messaging app—but the addition of WhatsApp's user base further solidified Facebook's dominance in the Social Advertising Market. More importantly, however, Facebook had removed a serious threat to its DTBE. If WhatsApp and its nascent social platform were allowed to compete on the merits, Facebook would not have been able to leverage its Platform into continued dominance of the Social Advertising Market, including by using API access to shut down competing third-party apps and to demanding access to other apps' most valuable social data as a condition for their existence.

301. Moreover, because the reach and engagement on WhatsApp generated (and generates) significant social data that Facebook could (and can) leverage and monetize through its mobile advertising channel, Facebook's DTBE strengthened as a result of the WhatsApp acquisition, fortifying Facebook's unrivaled dominance in the Social Advertising Market, and strengthening Facebook's ability to exclude potential entrants to this market from gaining a foothold with a rival messaging or photo-sharing app.

[illegible]

FILED UNDER SEAL

| Age Group | Number of Respondents |
|-----------|-----------------------|
| 1 | 100 |
| 2 | 100 |
| 3 | 25 |
| 4 | 100 |
| 5 | 100 |
| 6 | 100 |
| 7 | 95 |
| 8 | 65 |
| 9 | 65 |
| 10 | 40 |
| 11 | 40 |
| 12 | 45 |
| 13 | 50 |
| 14 | 35 |
| 15 | 35 |
| 16 | 100 |
| 17 | 100 |
| 18 | 100 |
| 19 | 35 |
| 20 | 100 |
| 21 | 100 |
| 22 | 100 |
| 23 | 85 |
| 24 | 35 |
| 25 | 35 |
| 26 | 40 |
| 27 | 50 |
| 28 | 0 |

[illegible]

FILED UNDER SEAL**A. The Aftermath of the Platform Change and the App Vacuum.**

316. After Zuckerberg made his announcement at F8 in April 2014, Facebook continued to allow access to the Newsfeed and Friends APIs for another year. By the end of April 2015, however, Facebook had finally withdrawn general access to the APIs, destroying tens of thousands of third-party apps on its Platform.

317. Facebook quietly exempted certain developers from its decision, hand-selecting developers from whom Facebook could obtain particularly valuable targeting data; developers that made large ad purchases, especially on Facebook's new mobile ad platform, NEKO; and developers that met both criteria.

318. Notwithstanding these exemptions, Facebook's third-party app ecosystem had been decimated. Where thousands of apps previously performed various functions on Facebook's Platform, allowing Facebook to obtain data from a broad ecosystem of third-party apps for its ad targeting, those apps were now gone—and so was the advertising revenue and user engagement those apps generated.

319. Facebook itself was now the principal (and for many types of user data, only) source of user data from its social network—from within Facebook's walled garden. Outside developers could, for the most part, no longer query Facebook's most valuable Graph social data through the Facebook Platform. Rather, Graph data was only available to Facebook and those that it hand-selected for access.

320. Among the apps with high amounts of engagement, Facebook had purchased two of the most successful apps with the fastest growing user bases, WhatsApp and Instagram. Facebook's core product also included Facebook's messaging app, Messenger. Facebook's control over these properties provided it with social data from important social networking vertical products and adjacent features—namely, mobile messaging and photo sharing.

321. With its Platform scuttled, Facebook would have to obtain engagement and social data from its own offerings, but Facebook lacked offerings in major categories, such as travel, e-commerce, streaming video, and location-based services. Facebook could no longer rely on third-party apps to obtain social data from user interactions in those spaces.

FILED UNDER SEAL

322. By April 2015, Facebook's priorities had accordingly shifted. It needed its own direct avenues of collecting user data from within its walled garden.

[illegible]

FILED UNDER SEAL

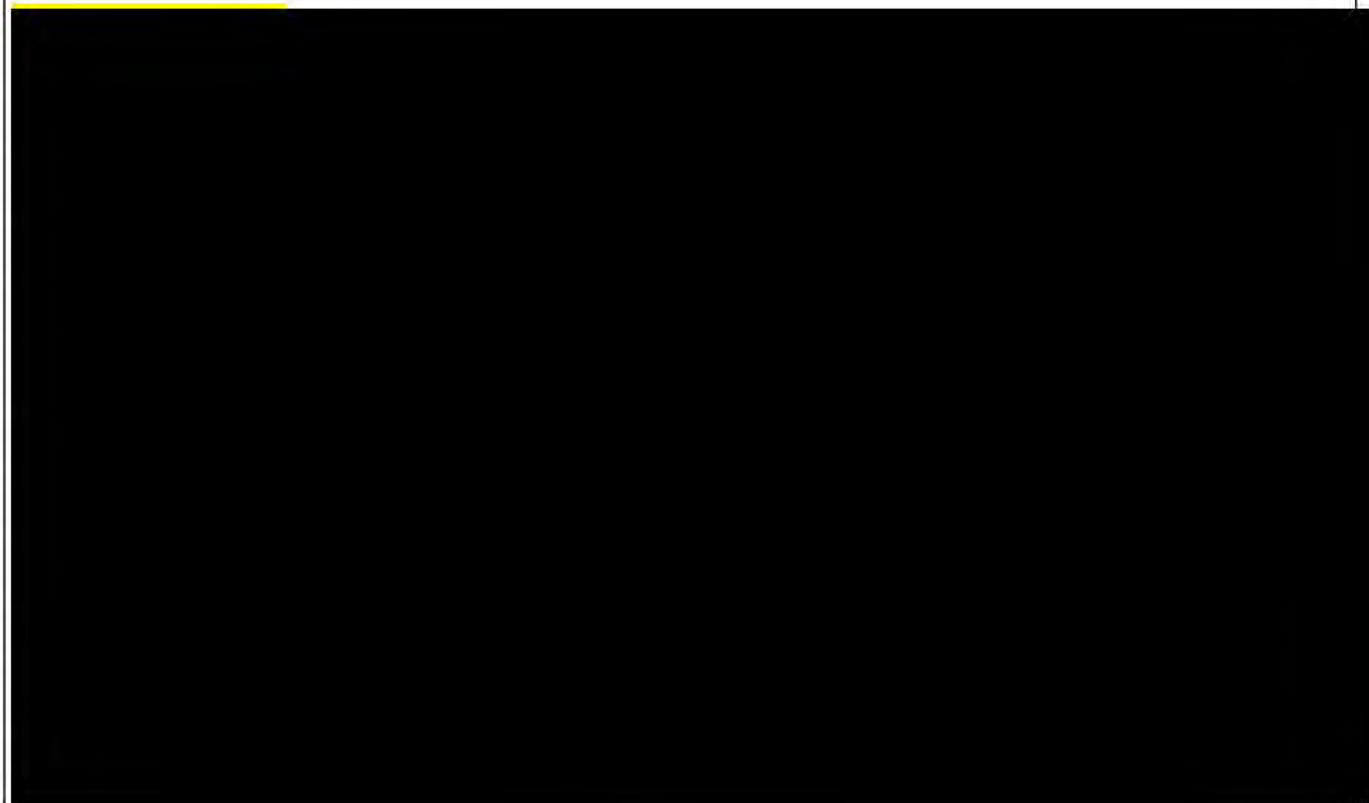
[illegible]

[illegible]

FILED UNDER SEAL

[illegible]

FILED UNDER SEAL



FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

[illegible]

[REDACTED]

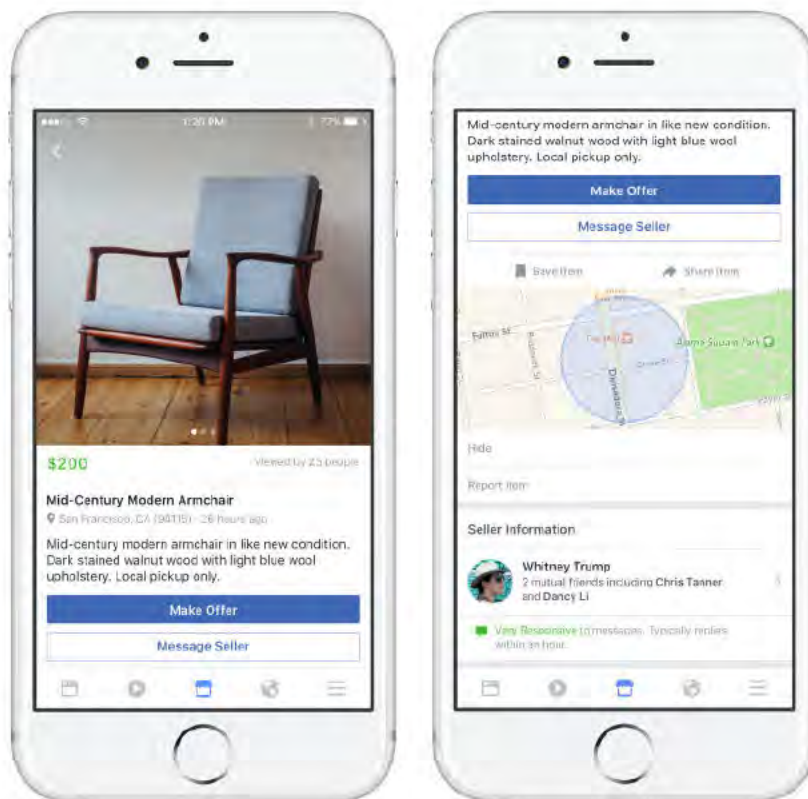
[REDACTED]

354. Facebook launched Marketplace on October 3, 2016, with a focus mostly on customer-to-customer transactions. The initial product was to compete with sites like Craigslist, but Facebook expected to expand its product to encompass sales from businesses. TechCrunch reported on Marketplace the same day as its launch, heralding the new functionality:

FILED UNDER SEAL

Facebook Marketplace lets you browse a relevancy-sorted feed of things to buy from people who live nearby, and quickly list your own stuff for sale. Integration with Facebook Messenger lets you haggle or arrange a meet-up, and you know more about who you're dealing with than on anonymous sites like Craigslist thanks to Facebook's profiles.

355. Facebook's Marketplace was launched as the central feature on Facebook's mobile product in 2016. In fact, Facebook placed an icon for Marketplace at the center of its mobile app's navigation bar.



356. TechCrunch noticed the prominence of the new feature. It was clear to the news outlet that Facebook was making a large bet on Marketplace:

Facebook is betting big on Marketplace, considering it's taking over a main spot in the navigation tab bar, replacing the Messenger shortcut in Facebook for iOS. That prime location could make Marketplace the digital version of impulse buys at the checkout counter.

FILED UNDER SEAL

| | |
|----|------------|
| 1 | [REDACTED] |
| 2 | [REDACTED] |
| 3 | [REDACTED] |
| 4 | [REDACTED] |
| 5 | [REDACTED] |
| 6 | [REDACTED] |
| 7 | [REDACTED] |
| 8 | [REDACTED] |
| 9 | [REDACTED] |
| 10 | [REDACTED] |
| 11 | [REDACTED] |
| 12 | [REDACTED] |
| 13 | [REDACTED] |
| 14 | [REDACTED] |
| 15 | [REDACTED] |
| 16 | [REDACTED] |
| 17 | [REDACTED] |
| 18 | [REDACTED] |
| 19 | [REDACTED] |
| 20 | [REDACTED] |
| 21 | [REDACTED] |
| 22 | [REDACTED] |
| 23 | [REDACTED] |
| 24 | [REDACTED] |
| 25 | [REDACTED] |
| 26 | [REDACTED] |
| 27 | [REDACTED] |
| 28 | [REDACTED] |

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FILED UNDER SEAL**D. Facebook Moves into Location-Based Services**

365. By the end of 2015, Facebook faced nascent competition from a growing location-based social network, Foursquare. Foursquare had expanded the concept of the social network to the physical world, allowing its users to “check in” at various locations, notifying friends of their whereabouts.

366. In July 2014, Foursquare had split itself into two apps—Swarm and Foursquare. Swarm would focus on location-based messaging, while the Foursquare app would focus on local recommendations based on a user’s location. Both apps threatened to make inroads on Facebook’s social networking business through innovations in location-based services.

367. Foursquare had laboriously developed the data required for its location-based social network, including information about places of interest, restaurants, shops, and other places frequented by its users. Foursquare provided this information to third-party integrators and apps through the Foursquare API. TechCrunch described Foursquare’s data, API, and network of integrators in a May 5, 2015, article:

Places by Foursquare, meanwhile, is the company’s repository of Places, a database of about 65 million points of interest that the company says can be used as an end-to-end location solution. This is the database that is built

FILED UNDER SEAL

1 out not just through the network of developers who use Foursquare's
2 API—which includes companies like Citymaps, Microsoft and Garmin—
but also through Foursquare's own apps.

3 368. Foursquare's database of Places gave it a running start against Facebook in the rapidly-
4 developing location-based services sub-vertical, and the company had aggressively built a competing
5 social network using that head start. In December 2015, Foursquare raised an additional round of funding
6 based on the premise that the data it had gathered was uniquely valuable.

7 369. But worse for Facebook than simply Foursquare's nascent social network was the
8 company's rich trove and pipeline of real-time socialized location data. Such data—which could
9 potentially be used to powerfully target social advertisements in the right hands—was imminently
10 licensable from Foursquare through its API, and this posed a significant potential threat to Facebook's
11 Social Advertising monopoly. If Foursquare's real-time location data repository and pipeline were
12 provided to a potential entrant at scale in Social Advertising—or Foursquare itself grew its Social
13 Advertising products with a valuable location-based data trove while Facebook was itself still preparing
14 for meaningful entry into location-based services, this could significantly erode the DTBE, as location-
15 based targeting and inferences and signals relating to location were on the verge of becoming perhaps the
16 most valuable targeting signals for social advertising.

17 [REDACTED] Unfortunately, Foursquare [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]
28

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FILED UNDER SEAL

[illegible]

FILED UNDER SEAL**E. Streaming Video and Facebook Watch**

379. Another potential source of user social data that could be mined for ad-powering targeting information was streaming video. By 2016, Facebook had included a video tab in its mobile product, but long-form and episodic videos were taking hold in the market—and formed a particularly rich source of potential social data targeting.

380. In 2017, Netflix was the pre-eminent streaming service that specialized in long-form television and movie content. Netflix's streaming service had grown significantly, from approximately \$8.8 billion in revenue in 2016 to \$11.6 billion in revenue in 2017.

381. Netflix was also a powerful source of user data. The movies, TV shows, clips, sports, and episodic videos its users watched and interacted with shed light on their interests, as well as their likely purchasing decisions.

382. At the heart of Netflix's service was its recommendation algorithms. Netflix's recommendation algorithm tailored content to particular users. As the Wall Street Journal explained in a November 10, 2018 article: "Analytics is deeply embedded in Netflix's DNA. The company mines reams of data on its subscribers' tastes to help determine which shows to bet on and how to promote them." Moreover, Netflix uses powerful AI and ML models to determine which shows and movies to license and what original programming to create.

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

[REDACTED]

[REDACTED]

26
27
28

FILED UNDER SEAL

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 388. Watch allowed video to be tailored to individual users, including based on their network
5 of friends and their habits. Facebook also curated video to users based on what others on its network were
6 watching. As TechCrunch explained in an article dated the same day as Watch's launch:

7 Watch features personalized recommendations of live and recorded shows
8 to watch, plus categories like "Most Talked About," "What's Making
9 People Laugh" and "Shows Your Friends Are Watching." Publishers can
10 also share their shows to the News Feed to help people discover them. A
11 Watchlist feature lets you subscribe to updates on new episodes of your
12 favorite shows. Fans can connect with each other and creators through a
13 new feature that links shows to Groups.
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20
21
22
23
24
25
26
27
28

FILED UNDER SEAL

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[illegible][illegible]

FILED UNDER SEAL**VII. FACEBOOK'S ENTRY AND DATA CAPTURE CONDUCT**

394. Facebook's business has long relied on selling advertising targeting users that interact with its properties, including Instagram, WhatsApp, Messenger, and its core Facebook product. As users actually interact with these products—*e.g.*, a user browses Instagram; chats via WhatsApp or Messenger; or navigates Facebook's website or mobile app—their identities are readily ascertainable by Facebook. These users are logged in to Facebook, and their every move tracked, logged, and converted into structured social data to be mined by Facebook's ML and AI systems.

By 2015, Facebook's users were using smartphones and web applications to perform time- and attention-consuming activities that Facebook had not made part of its owned-and-controlled product. Worse still, after the (pre-planned) demise of Facebook's open Platform in early 2015,

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FILED UNDER SEAL

1
2
3
4
5

14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

[REDACTED]

[REDACTED]

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

FILED UNDER SEAL

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 418. From 2015 to 2016, Facebook was in increasing competition with nascent social network
5 Foursquare. Foursquare's competitive edge—[REDACTED]
6 [REDACTED]—was its laboriously created
7 database and data stream of location data, including its users' real-time location social data.

8 419. Facebook moved directly into Foursquare's location-based corner of social networking
9 beginning in earnest on January 29, 2015, when it announced its own "Place Tips" product, directly
10 competing with Foursquare's location-based recommendation engine.

11 420. Facebook expanded further into Foursquare's territory in 2016 and 2017, putting further
12 pressure on Foursquare—which was rapidly raising capital to compete with Facebook.

13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED]

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[illegible]

101

[illegible]

First Amended Consolidated Advertiser Class Action Complaint – Case No. 20-CV-08570-JD

[illegible]

FILED UNDER SEAL

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

FILED UNDER SEAL

Stephanie, I think you should circulate the proposed term sheet to Dan

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

109

[illegible]

111

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

27
28

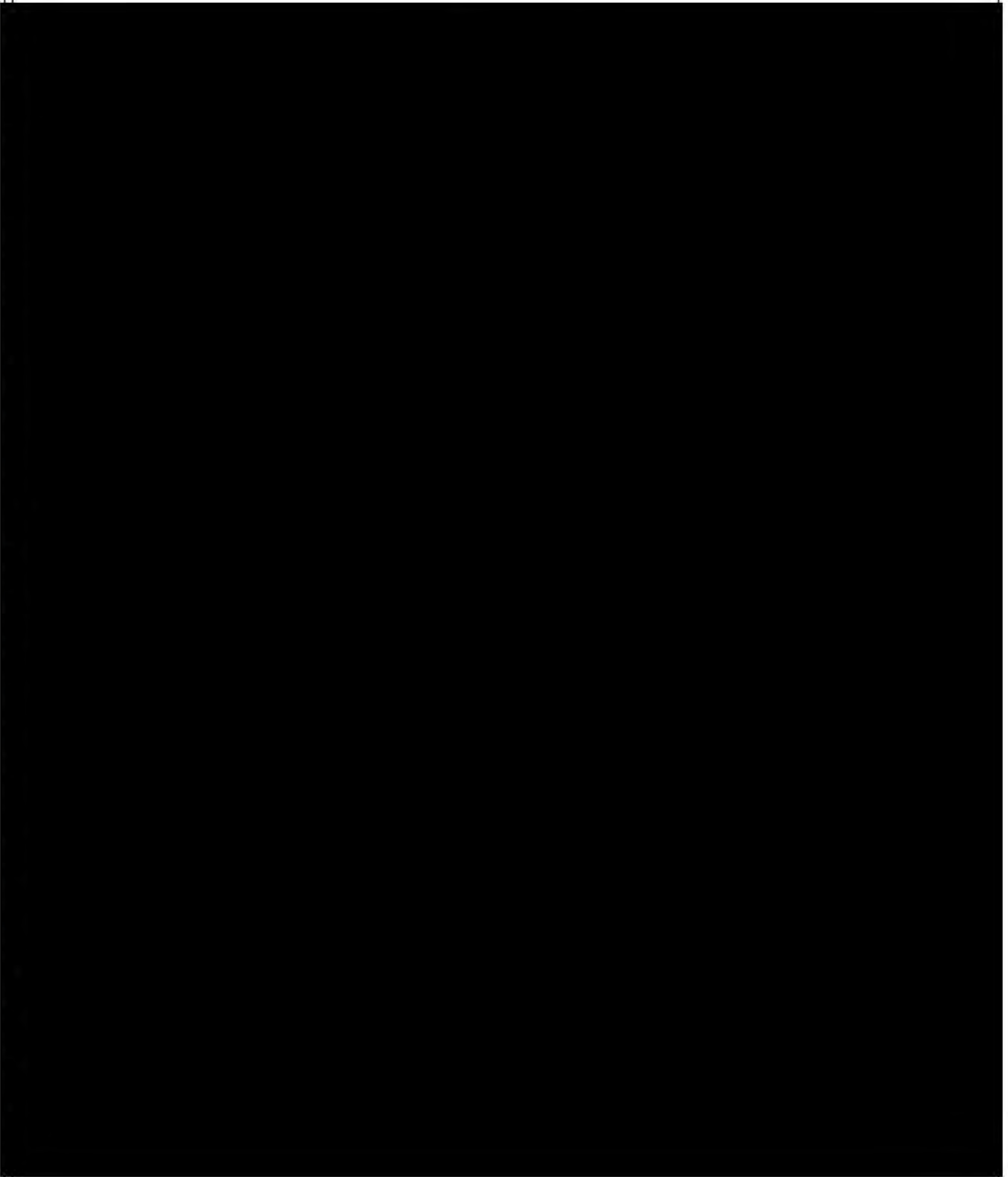
113

FILED UNDER SEAL

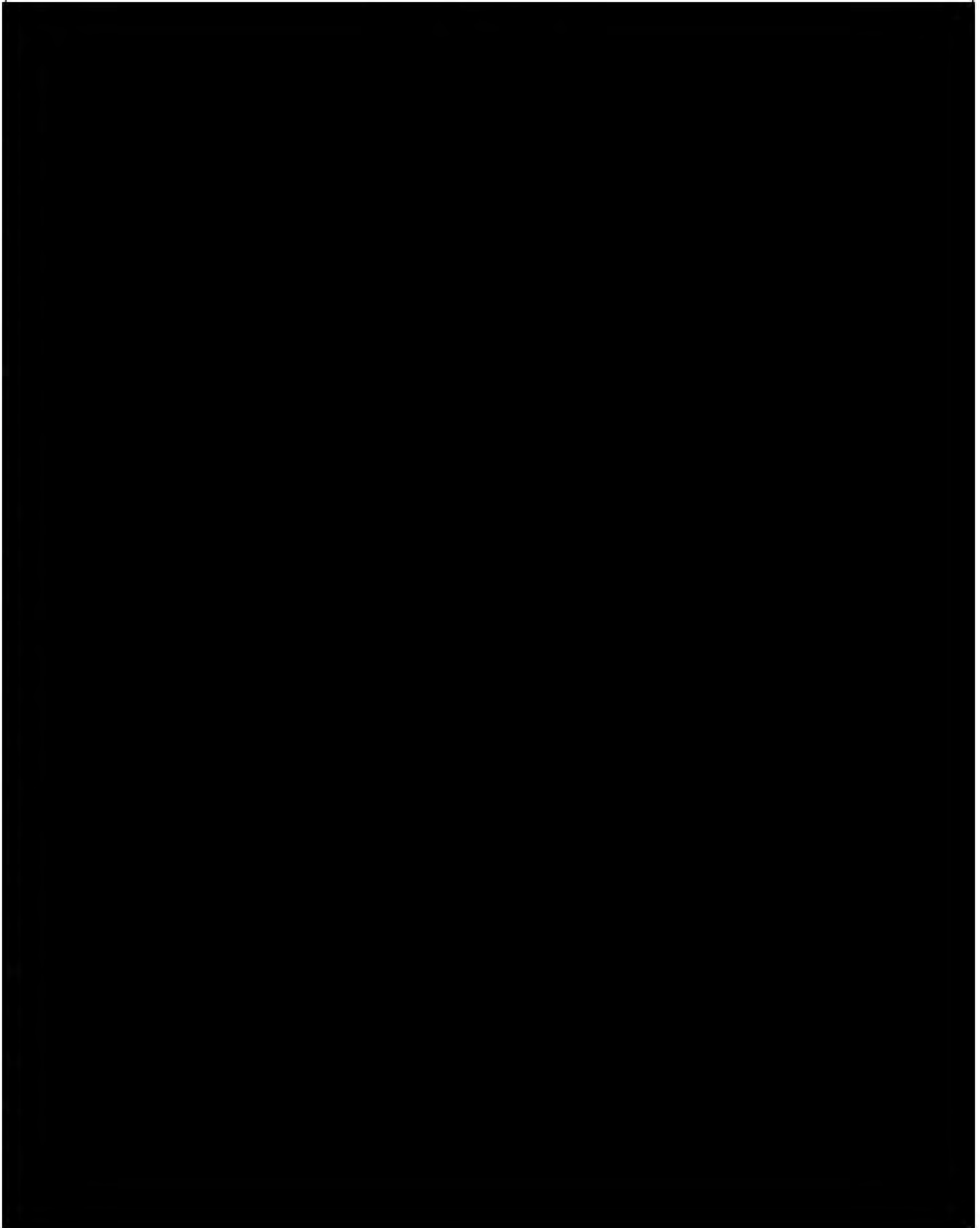
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

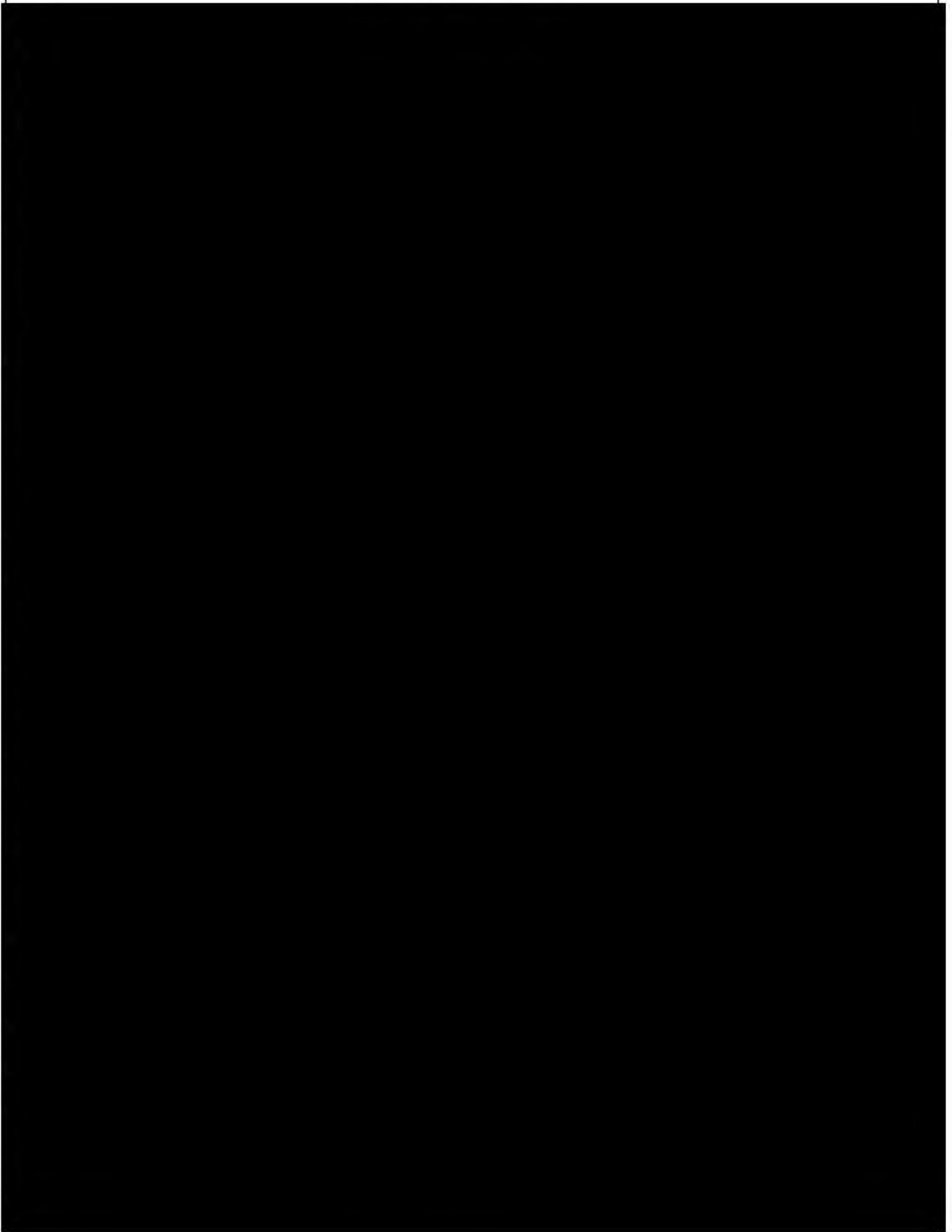
FILED UNDER SEAL



FILED UNDER SEAL

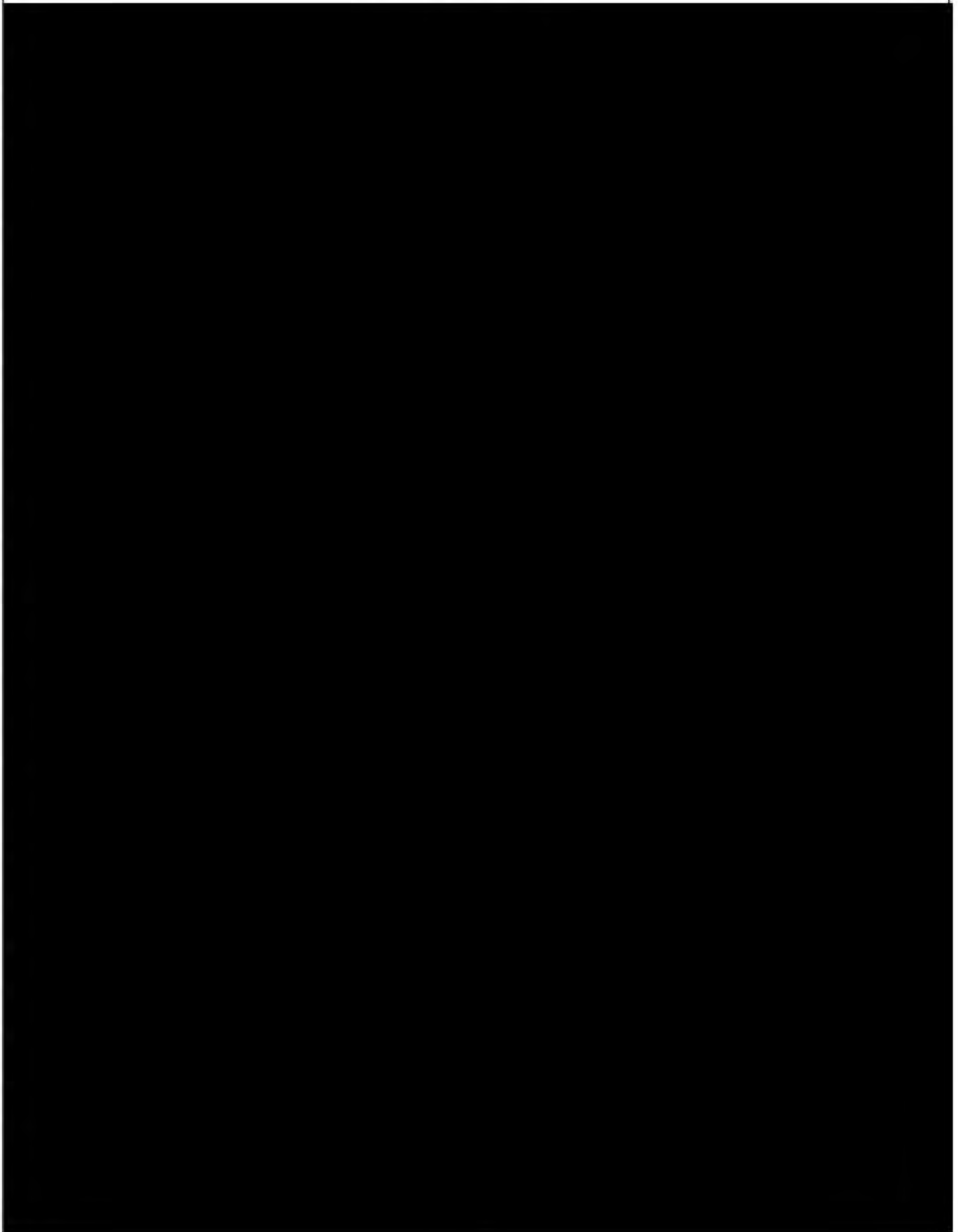


FILED UNDER SEAL



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FILED UNDER SEAL



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FILED UNDER SEAL

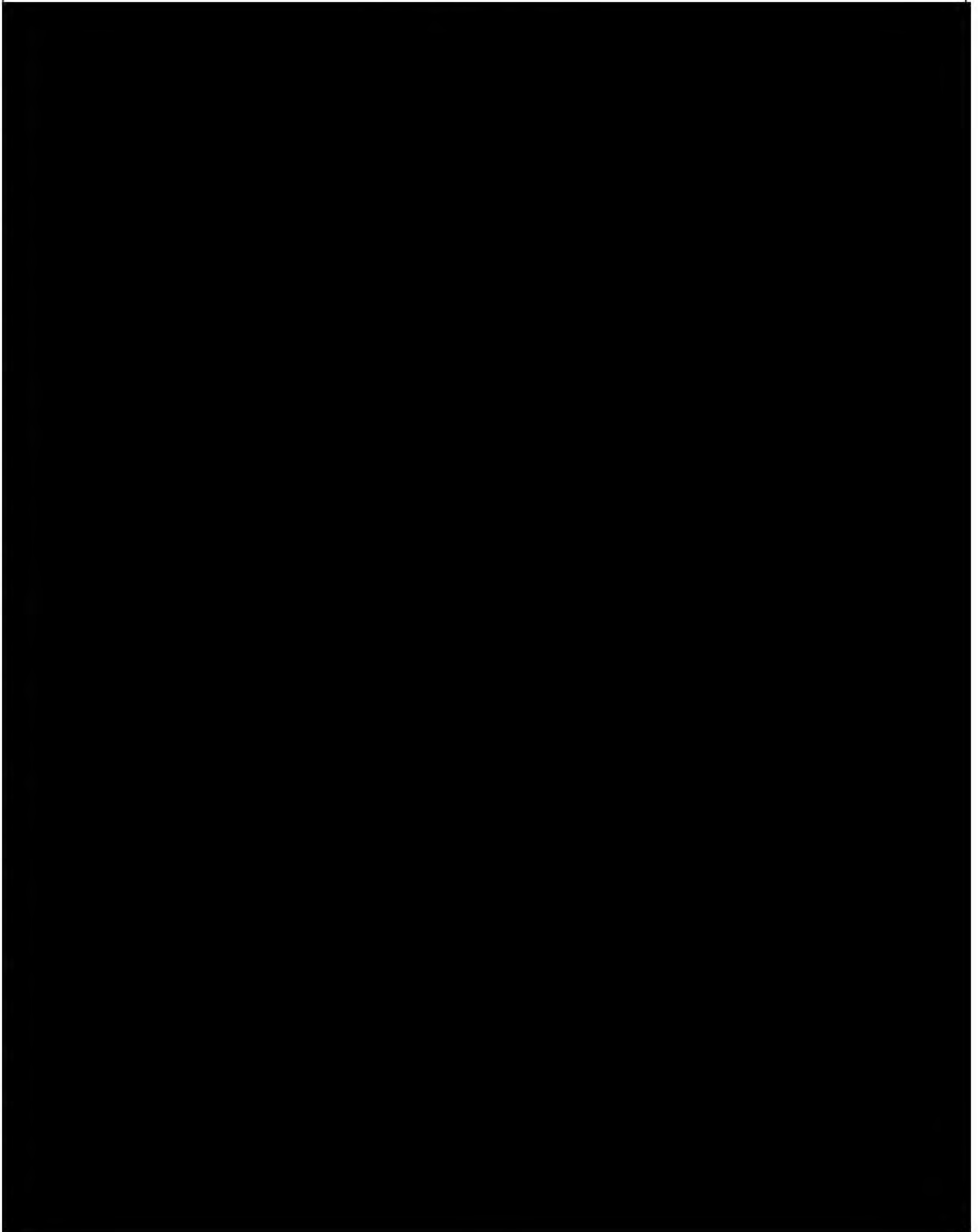
1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED]

[illegible]

[illegible]

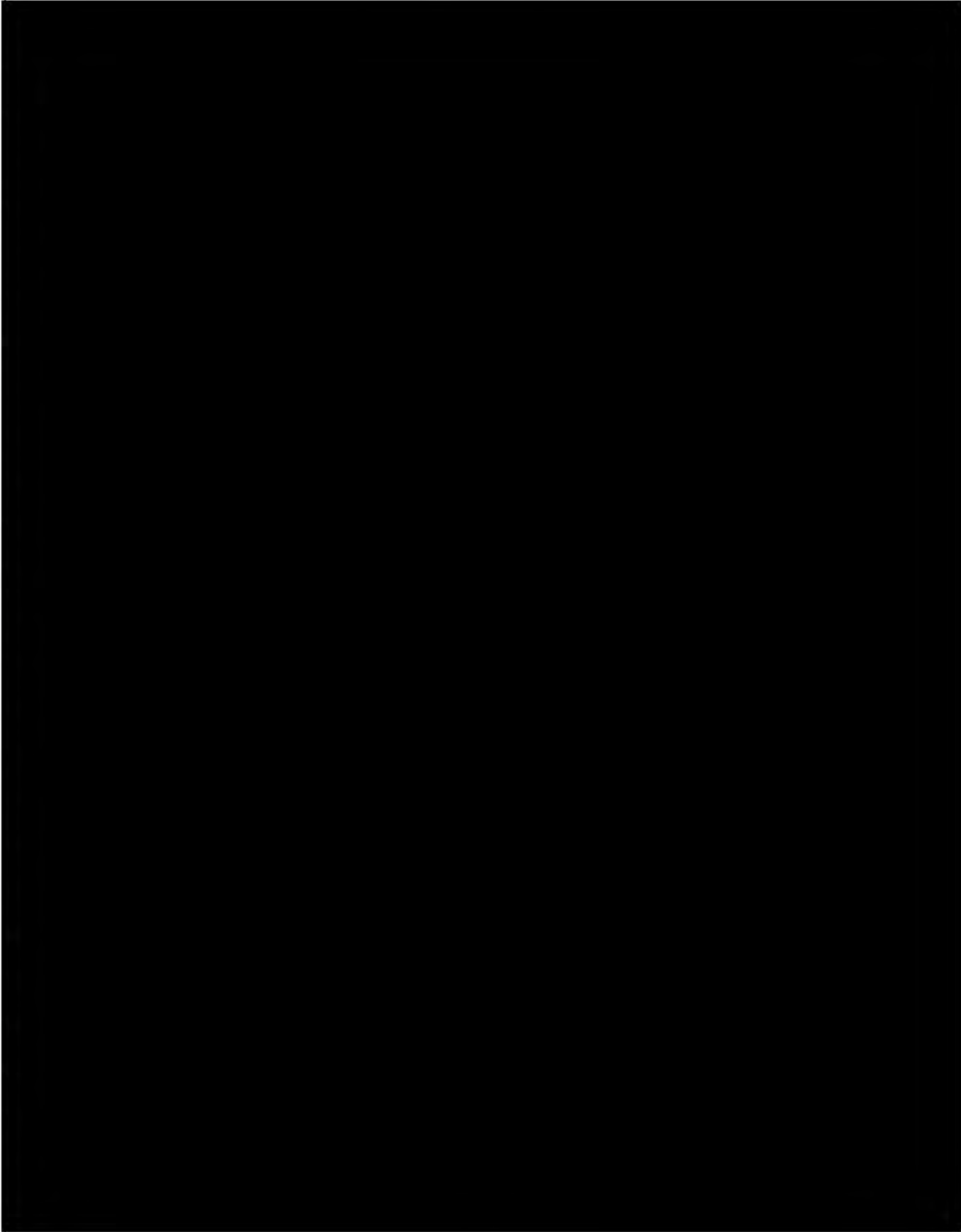
[illegible]

FILED UNDER SEAL



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FILED UNDER SEAL



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

First Amended Consolidated Advertiser Class Action Complaint – Case No. 20-CV-08570-JD

[illegible]

FILED UNDER SEAL

526. In December 2018, Facebook cut the funding for its news shows on watch. In February 2019, Facebook announced that it would not be renewing most of its news programs. As *Digiday* reported on February 26, 2019:

Last June, Facebook rolled out its first set of daily and weekly news shows from publishers such as ABC News, CNN, Business Insider and NowThis. Overall, Facebook has launched 21 news shows on Watch including CNN's "Anderson Cooper Full Circle," BuzzFeed's "Profile" and Univision's "real America with Jorge Ramos."

In recent months, Facebook has been telling news publishers that it will only renew about a third of the existing news shows that it has funded for Facebook Watch, according to publishing sources that have met with Facebook.

527. Facebook also began cutting its original content, particularly its scripted series. In January 16, 2020, Facebook cut popular shows *Sorry for Your Loss* which starred Elizabeth Olsen, and *Limetown* which was headlined by Jessica Biel.

528. By early 2020, Facebook had publicly canceled virtually every drama on its platform, including *SKAM Austin*, *Five Points*, *Sacred Lies*, *Turnt*, *The Birch*, and *Steroscope*. Facebook also cut its comedies, *Strangers* and *Queen America*. Facebook cut its docuseries, including *Humans of New York*:

FILED UNDER SEAL

1 *The Series, Bill Murray & Brian Doyle-Murray's Extra Innings, Tom vs. Time, Fly Guys, Behind the*
2 *Wall: Bubba Wallace, and Inside the Madness: Kentucky Basketball.*

3 529. Facebook cut its game shows, *Confetti* and *Outside Your Bubble*. Facebook also cut its
4 animation series, *Human Kind of*, *Liverspots and Astronots*, and *Human Discoveries*. Facebook cut
5 almost ever reality show, including *No Script with Marshawn Lynch*, *Relationships*, *Backcourt: Wade*,
6 *The Tattoo Shop*, *Bear Grylls: Face of the Wild*, *Help Us Get Married*, *Huda Boss*, *Sneaker Hustle*, *Troy*
7 *the Magician*, *You Kiddin' Me*, *Big Chicken Shaq*, *Double Take*, and *Will Smith's Bucket List*.

8 [REDACTED]

9 [REDACTED]

10 [REDACTED]

11 [REDACTED]

12 [REDACTED]

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 [REDACTED]

19 [REDACTED]

20 [REDACTED]

21 [REDACTED]

22 [REDACTED]

23 [REDACTED]

24 [REDACTED]

25 [REDACTED]

26 [REDACTED]

27 [REDACTED]

28 [REDACTED]

FILED UNDER SEAL

536. On April 12, 2019—

—Facebook announced that Reed Hastings would be leaving Facebook’s Board of Directors.

FACEBOOK ANTICOMPETITIVELY USED ONAVO DATA TO BUILD A MASSIVE, SURVEILLANCE SYSTEM AND TO SPY ON FACEBOOK USERS

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

[REDACTED]

FILED UNDER SEAL

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED]

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

[illegible]

FILED UNDER SEAL

[REDACTED]

569. This gave Facebook an immense advantage over competitors. While competing apps would have to obtain user data from their own apps, Facebook was able to capture user data from third-party apps in addition to its own. This directly strengthened Facebook's ability to target users for content and advertising, and it gave Facebook a real time view of potential competitive threats as well as the information and time Facebook's own users contributed to those threatening apps. This contributed to

FILED UNDER SEAL

and fortified the DTBE, helping maintaining Facebook's Social Advertising monopoly and injuring Plaintiffs and the proposed classes.

IX. THE THREAT BEYOND FACEBOOK'S WALLED GARDEN

570. To maintain its dominant position in Social Advertising, Facebook would have to ensure its ability to granularly target Facebook users. But because those users spent significant time outside of Facebook, including on mobile apps and web applications, Facebook needed to effectively harvest social data from them even when they were not on Facebook. And, to maintain the competitive edge it enjoyed from its DTBE, Facebook would have to extend its ability to target users outside of its walled garden.

A. Facebook Audience Network

571. Facebook announced a new advertising system at the 2014 F8 conference in April of 2014 called the Facebook Audience Network ("FAN"). FAN allowed developers to target both standard banners and custom ad units using Facebook's vast trove of personal data. Advertisers would be able to buy ad space in mobile applications through FAN, and developers could purportedly monetize their apps.

572. As TechCrunch reported ahead of the F8 announcement, FAN would allow advertisers to use Facebook's granular targeting system to advertise in mobile applications:

Facebook will also bring the ad targeting muscle, allowing advertisers to reach people based on biographical and interest data, and likely with cookie-based retargeting, too. Most other ad networks have a limited amount of data regarding who someone is, and that data is often inferred so it's not always accurate. That makes it tougher meaning to show relevant ads that get results and command high rates for publishers. *[sic]*

But Facebook's social network has convinced people to volunteer tons of deep personal information like work history, education, and favorite movies, plus it can see what apps they use and where they are. Since people stay logged into Facebook, FAN can recognize exactly who the viewer is and show them an ad matched to their profile.

573. Part of Facebook's focus was on developers, as they were Facebook's largest mobile ad customer because they sought new users through app installs. FAN would provide new forms of advertising, including early forms of advertising "retargeting"—reengaging with a user after an ad impression or other event. As TechCrunch explained:

FILED UNDER SEAL

1 The ads themselves could promote a range of products. There's sure to be
2 plenty of app install ads, Facebook's current cash cow, as developers are
3 desperate for installs and willing to pay. Mobile app-reengagement ads
4 could also be popular. You might already have Hotel Tonight installed, but
5 have forgotten about it. If Facebook sees you like traveling, and just
6 checked in to a restaurant in Los Angeles, it could show an ad delivered
7 through FAN in another app that re-opens HotelTonight to a \$99 hotel
8 room in the city. Big brands and local businesses might also get in on the
9 action, as Facebook's offline measurement tools can prove that its ads drive
10 in-person sales.

11 574. Facebook was opening up an entirely new class of features—those dependent on tracking
12 users across devices and apps.

13 575. FAN went live in October 2014, and what was launched was significantly broader than
14 what Facebook had announced at F8. FAN was not released as a separate advertising stream. Instead, it
15 was implemented as an extension of Facebook's existing advertising system. This meant that a Facebook
16 Ad, using Facebook's granular targeting systems, could be used to target ads outside of Facebook's
17 properties—directly in third-party, mobile apps.

18 576. TechCrunch covered the new functionality, explaining its significance:

19 Until now, each dollar Facebook earned meant annoying its own users with
20 more ads. This created a natural cap on Facebook's revenue unless it
21 wanted to pester us so much that we stopped visiting. Now it can sit back
22 and cash in on all the targeting data it's collected.

23 577. Facebook had created finely tuned machine-learning systems to target users by, among
24 other things, biographical and interest-based information it had collected about them as they interacted
25 with other Facebook users. Those machine-learning algorithms would now be turned loose outside of
26 Facebook's walled garden, allowing them to granularly target and track Facebook's users even when they
27 were using someone else's mobile application.

28 578. The value of this new functionality was not just the ability to display ads on mobile
applications that Facebook did not control—it also provided Facebook more critical user data, particularly
social data, which its machine-learning algorithms needed as fuel. Facebook would be able to learn more
about its users, including how they interacted with other users and content outside of Facebook,

FILED UNDER SEAL

Instagram, or WhatsApp. This made Facebook better at serving both content and advertising to users while on Facebook-controlled apps, reinforcing the DTBE.

579. Initially, Facebook's Login product, which it had promoted at F8 2014, was one of the ways Facebook was able to track users across applications. Users who logged into a third-party app using their Facebook login were then tracked by Facebook as they used those apps.

580. In May 2016, however, Facebook extended FAN even further, to track Facebook users who were not even logged into Facebook. As Facebook explained in a blog article:

Over the coming months we will expand the reach of Facebook-powered advertising on the Audience Network to include people who don't have accounts. To ensure that the ads people see in the apps and websites in the Audience Network are highly relevant, we will use information we receive from third-party sites and apps that use Facebook technology.

581. On May 27, 2016, the *Wall Street Journal* reported that the change allowed tracking of users across the Internet, positioning Facebook to compete head-on with Google:

To that end, the social network and online advertising company said Thursday it will now help marketers show ads to all users who visit websites and applications in its Audience Network ad network. Previously Facebook only showed ads to members of its social network when they visited those third-party properties.

The change is a subtle one, but it could mean Facebook will soon help to sell and place a much larger portion of the video and display ads that appear across the Internet. The change will also intensify competition with Alphabet Inc. subsidiary Google, which dominates the global digital-advertising market, and a wide range of other online ad specialists.

582. Facebook now planned to leverage its targeting systems outside its walled garden. It would monitor users who were not logged into Facebook at all, allowing FAN to extend Facebook's edge beyond the Social Advertising Market, which it had dominated by virtue of the DTBE protecting its business.

B. Facebook Acquires Atlas

583. On December 6, 2012, news broke that Facebook was considering acquiring a company called Atlas from Microsoft. Atlas was a software company that both served ads and tracked ad conversions.

FILED UNDER SEAL

584. For example, Atlas technology would log when a user viewed an ad that was served to them, and then if they later, for example, purchased a product (that is, the ad “converted”), Atlas technology would allow attribution of the sale to the advertisement.

585. Google had paid \$3 billion dollars for its own ad-serving product, DoubleClick, in 2007. Although Atlas lacked the sophistication of DoubleClick—particularly after Google had developed and integrated the DoubleClick software with its own—the purchase of Atlas positioned Facebook to grow and extend its capability to granularly target users with advertising well beyond Facebook’s own properties.

586. In Facebook’s hands, however, Atlas and its technology was even more valuable. As Business Insider explained in December 2012:

The value of a Facebook-powered/Atlas-supported ad network could be tremendous.

Here’s why.

Facebook is the only company in the world that has a billion email addresses, home addresses, and phone numbers on file.

This asset allows Facebook to do something no other Website can.

Facebook can tell marketers whether or not a Facebook user saw, on Facebook.com, an ad for a product before going to the store and buying it.

This is possible because retailers often have their shoppers’ phone numbers, home addresses, or email addresses on file. (They buy them from data collection companies.)

In the short term, Facebook will use this process to tell marketers exactly how much their sales increased thanks to ads on Facebook.com.

587. Acquiring software that could track conversions of Facebook ads outside of Facebook’s walled garden was a powerful extension of Facebook’s targeting apparatus. It closed feedback loops for events that occurred outside of Facebook’s view.

588. This ability, however, was about much more. Facebook’s DTBE stems both from the data it harvests from its users and the power of its machine-learning models, which consume that data. As users spend more time outside of Facebook’s properties, those machine-learning models have less to train

FILED UNDER SEAL

on, reducing the effectiveness of Facebook’s targeting. This in turn reduces engagement within Facebook, and as a result, the value of its targeted advertising. Facebook understood this threat in the early 2010s, with the rise of mobile apps. That is why it was—and remains—vital for Facebook to be able to track its own users when they are not using the core Facebook product, Instagram, or WhatsApp.

589. At its purchase, Atlas already had the necessary functionality, allowing advertisers to plan campaigns, buy ads on sites across the web, and measure their impact. It handled rich media and in-stream video, display ads, and offered APIs for programmatic control.

590. Internally, Facebook saw Atlas as a means to massively increase Facebook’s targeting capabilities. As Amin Zoufonoun, Facebook’s Vice President of Corporate Development, described to Sheryl Sandberg when Facebook was considering the acquisition, it gave Facebook “immediate scale to retarget, provide premium insights, do look-alike modeling, prove and measure efficacy of [Facebook] as a marketing medium, [and] enhance customer audiences and associated revenue.”

591. Most importantly, it gave Facebook the ability to use identity-based targeting through Facebook Identity—Facebook’s unique identifier for Facebook users across all browsers and devices—to serve highly targeted ads. Indeed, Facebook had described the value of Facebook Identity as the ability to “target people across browsers and devices” and to “[a]ctivate offline data to enrich online targeting,” among other features.

592. On February 28, 2013, Facebook acquired Atlas for approximately \$100 million. In its summary of the deal at the time of the transaction, Facebook noted that the transaction was an opportunity to become the “buy-side desktop tool that media planners fire up first thing in the day” and to acquire “a deep installed base of pixels which we can immediately turn on to power conversion tracking and attribution across offerings.”

593. The latter was the most important. By pixels, Facebook was referring to embedded web resources that would automatically pull information from a Facebook server when a user visited a non-Facebook site. Sometimes, this would be done through an invisible, single-pixel image, which would download from a centralized server. When the single-pixel image appearing on a third-party site was

FILED UNDER SEAL

downloaded by a user, Facebook would immediately know and would have the user's browser information, IP address, and device information as a result.

594. On September 29, 2014, Facebook announced through a blog post by Atlas's Managing Director Erik Johnson that Facebook had rebuilt Atlas "from the ground up," meaning that it had integrated it with its Facebook advertising systems. Facebook made the announcement ahead of Advertising Week in New York City.

595. Although Facebook removed the blog post and announcement from its site, *Wired* magazine contemporaneously recounted the focus of the announcement: unlike Google, Facebook would not need Cookies to identify users; it had its own data and targeting systems, which it had trained and honed using user interactions with its own properties:

In an apparent dig at Google, Johnson writes that the method advertisers have traditionally used to track consumers—cookies—is flawed, because consumers are no longer using one device at all times. "Cookies don't work on mobile, are becoming less accurate in demographic targeting and can't easily or accurately measure the customer purchase funnel across browsers and devices or into the offline world," Johnson writes. He offers "people-based marketing," that is, marketing based on Facebook's data, as the solution. It can not only track users between devices, but it can also connect online campaigns to offline sales to determine how effective a given campaign really was.

596. Johnson spoke at the Web Summit 2014 convention on its first day, November 4, 2014 (pictured below).



FILED UNDER SEAL

1 597. The focus of Johnson’s Web Summit talk was identifying users across devices and
2 throughout the Internet by using Facebook’s user targeting technology:

3 If that email address corresponds to an email address you use on Facebook,
4 we can now stitch together ads you’ve seen anywhere on the internet with
5 a purchase you made in a store. Facebook has had this functionality for
6 some time now, but with Atlas, we’re able to take the cross-device, and the
7 people-based and the offline-to-online story that Facebook has and move
8 it to the rest of the internet.

9 598. Atlas gave Facebook the ability to leverage and extend its DTBE. Facebook could not only
10 target users as they interacted on Facebook-controlled applications, but when they interacted with other
11 apps and websites. This sharpened Facebook’s own targeting across its properties.

12 **C. Facebook Positions Itself Against Google by Combining Atlas, Audience Network,
13 and Other Technology**

14 599. By December 10, 2014, Facebook had acquired several key systems that positioned it to
15 extend its targeting advantage beyond Facebook’s products. In addition to Facebook Atlas and FAN,
16 Facebook had also acquired LiveRail for approximately \$400-500 million.

17 600. LiveRail connected marketers to publishers on web and mobile to target seven billion
18 video ads to visitors per month. It provided for real-time bidding, meaning that it dynamically matched
19 advertisement inventory with bids from marketers to optimize both revenue and effectiveness of that
20 advertising.

21 601. The technology Facebook acquired from LiveRail and Atlas, coupled with FAN, together
22 positioned Facebook to expand its dominance beyond its walled garden (Facebook’s three primary
23 products—Facebook itself, Instagram, and WhatsApp). Facebook’s advertising could reach beyond those
24 apps, tracking users across mobile devices and websites, and using information it gleaned from that
25 tracking to sharpen Facebook’s targeting algorithms within its own products.

26 602. The press likened the combined assets to an “AdTech Voltron,” a cartoon robot that
27 assembled a powerful robot out of smaller pieces:

28 Here’s how the pieces come together.

FILED UNDER SEAL

Facebook brings its 1.35 billion users and massive engagement with the News Feed where it shows its ads. Because its huge user base stays logged in across web and mobile, it has a unified understanding of people's identities in a way most platforms don't. Facebook's wealth of personal data means it can target ads more accurately. For instance, it says it can target gender with 90 percent accuracy compared to the online ad industry average of 50 percent.

603. The combination of these properties reinforced Facebook's primary form of leverage in the Social Advertising Market—its ability to granularly target users and to do so with significantly more accuracy than any other competing product. By tracking Facebook users both inside and outside of its walled garden, Facebook's targeting system was poised to span the Internet, mobile applications, and Facebook's social applications, including Instagram and WhatsApp.

604. Through a combination of these assets, Facebook was able to create "Lookalike Audiences," a new product announced in March 2013 that allowed Facebook to use its combined tracking information to train its machine learning algorithms to serve ads more likely to "convert" or otherwise result in desired feedback. Facebook could use a tracking pixel on a third-party site to find users within its own applications similar enough to likewise convert on the same site.

605. Facebook itself provides an example on its website:

Say you're an online florist that wants to reach people similar to those that made purchases on your website. Now you can use data from your Facebook pixels (Facebook Conversion Pixel or the Custom Audiences for Websites Pixel) to reach people who are most similar people who previously made purchases on your website.

606. Facebook boasted that e-commerce company Shopify "saw a 2x decrease in cost per lead when using lookalikes of their website visitors."

607. The new method of targeting advertisements meant that Facebook's machine learning was becoming more powerful—capable of self-tuning ad campaigns to maximize their effectiveness. After Facebook's ads had run for a while, they would become more effective without the need for manual user input. Facebook's machine-learning algorithms would optimize not only the ad, but Facebook's revenue. All the while, Facebook's algorithms would harvest more information from the users it tracked, allowing

FILED UNDER SEAL

it to further train its machine-learning models. This created a virtuous circle, expanding Facebook's targeting and trove of social data. The net result was a further strengthening of the DTBE.

D. Shadow Profiles and Identifying Users Outside of Facebook's Apps

608. Facebook's new strategy hinged on identifying its own users outside of Facebook's apps. By tracking those users outside of Facebook's walled garden, Facebook became better at targeting them within.

609. That is, by becoming better at serving content to users based on their web browsing or mobile app usage, Facebook could lock users into its own apps, reducing the need for them to leave Facebook apps while on the internet, which in turn made Facebook ads served to its own users significantly more effective than other forms of advertising.

610. Facebook needed a way to keep track of what users did across mobile applications, its own applications, and across the web. It did so by maintaining "shadow profiles" on users.

611. On April 16, 2018, after significant scrutiny before Congress, Facebook revealed the sources of the shadow profile data it collects:

When does Facebook get data about people from other websites and apps?

Many websites and apps use Facebook services to make their content and ads more engaging and relevant. These services include:

- Social plugins, such as our Like and Share buttons, which make other sites more social and help you share content on Facebook;
- Facebook Login, which lets you use your Facebook account to log into another website or app;
- Facebook Analytics, which helps websites and apps better understand how people use their services; and
- Facebook ads and measurement tools, which enable websites and apps to show ads from Facebook advertisers, to run their own ads on Facebook or elsewhere, and to understand the effectiveness of their ads.

FILED UNDER SEAL

1 When you visit a site or app that uses our services, we receive information
2 even if you're logged out or don't have a Facebook account. This is because
3 other apps and sites don't know who is using Facebook.

4 612. Facebook confirmed its information gathering in its written answers to the United States
5 Senate on June 11, 2018, admitting that Facebook collects extensive data even if a user is not logged into
6 a Facebook account.

7 613. All of this meant that Facebook was uniquely poised to expand and leverage its position
8 in the Social Advertising Market to challenge Google directly in online search and display advertising,
9 where Google had long established a dominant position. As explained in the next section, Facebook never
10 did so. Instead, it made an anticompetitive bargain with Google to preserve the Social Advertising
11 Market—and Facebook's dominance within it.

12 **X. FACEBOOK AND GOOGLE AGREE NOT TO COMPETE AND TO FORTIFY THE**
13 **FACEBOOK-DOMINATED SOCIAL ADVERTISING MARKET**

14 614. Although Facebook was poised to expand its advertising and targeting business beyond
15 its social networking apps, it never meaningfully did so. Instead, as explained below, it made a bargain
16 with Google that would help Facebook sharpen its machine-learning algorithms so that it could maintain
17 its superior ability to target its own users. In exchange, Facebook never challenged Google's dominance
18 outside of the Social Advertising Market.

19 **A. Google's Dominance Over Ad Exchanges and Ad Servers and the Looming**
20 **Facebook Threat**

21 615. As Facebook was taking its first steps outside of its walled garden, Google had already
22 achieved longstanding dominance in a form of advertising that allowed dynamic matching of display ad
23 inventory on websites and apps with marketers seeking to advertise to particular demographics.

24 616. Publishers provided their advertising inventory to Google's Ad Manager ("GAM"), which
25 would then either match that advertising inventory with a purchaser who had made a direct deal for
26 advertising or serve the available inventory to an ad exchange, where marketers bid for the inventory in
27 real time.

28 617. As an example, an online newspaper might have a space available on its site for an
advertisement. It would convey that information to an ad server, which would in turn find a buyer for the

FILED UNDER SEAL

1 space. In some cases, the ad server would send the available space to ad exchanges, which would sell the
2 ad space to the highest bidder.

3 618. By the mid-2010s, Google's ad server had become ubiquitous. Publishers, such as USA
4 Today, ESPN, CBS, Time, Walmart, and Weather.com, used (and still use) GAM. Today, GAM controls
5 over 90 percent of ad inventory from publishers.

6 619. Because most publishers use GAM to sell their inventory, Google serves as a middleman
7 to all the advertising exchanges, where bids from marketers are matched in real time with available
8 advertising inventory.

9 620. In addition to controlling the dominant ad server, Google also runs its own ad exchange,
10 called Google Ad Exchange or "AdX." Google charges an exchange fee for matching purchasers with ad
11 inventory, much of which comes through Google's dominant GAM.

12 621. Google's unique vantage point provides it with the ability not only to control the inventory
13 provided to exchanges, but to win bids against other ad exchanges.

14 622. That is, Google tracks website use through its analytics product. It tracks users on its Gmail
15 product. It tracks users when they use Google News. It even provides free DNS servers, resolving IP
16 addresses and web addresses for users across the internet. Google also has a unique vantage point because
17 of its mobile operating system, Android.

18 623. In recent years, Google's unique tools and properties have made it increasingly better-
19 suited to do what no other advertising exchange can do: identify who the person that visited a publisher's
20 website actually is, *i.e.*, their true, unique identity. Google's ad server and exchange are provided with
21 basic information about the person visiting the publisher's site, such as IP address, device identification
22 information, or browser information. Google's other tools and properties have increasingly positioned it
23 to do make granular identity determinations from this data.

24 624. In short, by the mid-2010s Google's advertising ecosystem was getting better and better
25 at doing something that Facebook had built its entire ad business upon, but could not outside of its own
26 properties—ascertain identity. (And, of course, Google could not, and cannot, serve ads to Facebook's
27 users on its properties.) By late 2016, with the rise of new technology and carefully targeted information
28

FILED UNDER SEAL

1 gathering properties like Android, Google’s ad products threatened to encroach upon Facebook’s
2 identity-focused ad targeting products—and indeed threatened to superset the Social Advertising Market
3 itself by allowing user and identity targeting outside of Facebook’s social network.

4 625. As Google’s capabilities increased, the prospect of a new, highly targeted form of
5 advertising emerged—one that could rival the effectiveness of buying advertising in the Social
6 Advertising Market, where Facebook was dominant and had unrivaled information about its users.

7 626. At the same time, Facebook became increasingly better in the mid-2010s at identifying
8 user identities and demographic information even outside of its own apps. Through Facebook’s series of
9 acquisitions, it was able to target users with its advanced machine-learning, even if the users were not
10 logged into Facebook.

11 627. By 2018, Facebook was a threat to leverage its technology into Google’s territory,
12 including by selling advertising in real-time in mobile applications and on the web. And Google’s rapidly
13 growing prowess in discerning identity was an existential threat to Facebook’s DTBE.

14 628. The two solved their problem by coming to an anticompetitive agreement code-named
15 “Jedi Blue,” as explained later in this Complaint. However, to properly understand the true stakes and
16 context of the once-looming clash of advertising titans, it is critical understand the role of AI and machine
17 learning tools in online advertising—and how these tools were differently wielded by Google and
18 Facebook in the run-up to their 2018 agreement to divide markets.

19 **B. Google’s AI Dominance**

20 629. Unlike Facebook, Google spent the 2010s becoming preeminent in machine learning and
21 artificial intelligence. For example, Google acquired groundbreaking AI technology when it purchased
22 UK-based DeepMind in January 2014 for more than \$500 million. And Google has leveraged this and
23 other bleeding-edge machine learning technology throughout its entire ecosystem ever since.

24 630. Google’s machine-learning dominance has allowed it to leverage its large cross-section of
25 user data across the Internet and mobile applications in increasingly powerful ways. For example, on
26 December 14, 2016, Google announced that it had used DeepMind technology to make recommendations
27
28

FILED UNDER SEAL

on its Google Play Store—Google’s mobile app store for Android devices. Google explained the problem and its AI-based solution on its AI blog:

Providing useful and relevant app recommendations to visitors of the Google Play Apps Store is a key goal of our apps discovery team. An understanding of the topics associated with an app, however, is only one part of creating a system that best serves the user. In order to create a better overall experience, one must also take into account the tastes of the user and provide personalized recommendations. If one didn’t, the “You might also like” recommendation would look the same for everyone.

Discovering these nuances requires both an understanding what an app does, and also the context of the app with respect to the user. For example, to an avid sci-fi gamer, similar game recommendations maybe of interest, but if a user installs a fitness app, recommending a health recipe app may be more relevant than five more fitness apps. As users may be more interested in downloading an app or game that complements one they already have installed, we provide recommendations based on app relatedness with each other (“You might also like”), in addition to providing recommendations based on the topic associates with an app (“Similar apps”).

One particularly strong contextual signal is app relatedness, based on previous installs and search query clicks. As an example, a user who has searched for and plays a lot of graphics-heavy games likely has a preference for apps which are also graphically intensive rather than apps with simpler graphics. So, when this user installs a car racing game, the “You might also like” suggestions includes apps which relate to the “seed” app (because they are graphically intense racing games) ranked higher than racing apps with simpler graphics. This allows for a finer level of personalization where the characteristics of the apps are matches with the preferences of the user.

631. Google thus tackled a problem Facebook had solved socially (with actual social data), but did so in a different way—by using complex machine learning that did not require social signals to make social evaluations and recommendations. Rather than collecting actual friend recommendations and activity, Google used machine learning—*i.e.*, deep neural network models—to study a user’s decisions and preferences, then identified that other apps that might interested that user.

632. Facebook, on the other hand, had monetized app installs for years—Facebook’s “cash cow”—by using its social targeting systems to traverse its network and coax other users to install apps

FILED UNDER SEAL

1 using social connections. Facebook used social data, data about its users' interactions within its social
2 network, to devise and train machine-learning algorithms that would make predictions about who would
3 be interested in installing an app.

4 633. It was this "recommendation engine" technology that was at the center of Zuckerberg's
5 concerns about Tinder during Facebook's early 2010s API scheme. Indeed, in January 2014, Zuckerberg
6 was concerned that "recommendations seems like something that should be right up our alley," but was
7 "something we're not very good at." He found Tinder's growth "alarming" because its recommendation
8 engine was "built completely on Facebook data" and was "much better than anything we've built for
9 recommendations using the same corpus."

10 634. But as Facebook sought to expand its machine-learning capability outside of its walled
11 garden, it faced a Google that was far ahead of it in the field of artificial intelligence and machine learning.
12 This meant that Google was better at identifying users, and if left unchecked, would be better at targeting
13 Facebook's own users throughout the Internet, including on mobile applications.

14 **C. The Rise of Header Bidding and Facebook's Threat to Compete with Google**

15 635. By 2016, a competitive collision between Facebook and Google looked imminent.
16 Facebook was well positioned to move into the ad exchange business, and Google was poised to break
17 Facebook's dominance over granular, identity-based ad targeting, including within long-siloed social
18 networks such as Facebook, Instagram, and WhatsApp.

19 636. The threat of competition heightened in 2015 and 2016 when publishers began to adopt a
20 practice called "header bidding." Header bidding routed ad inventory to multiple neutral exchanges each
21 time a user visited a web page in order to return the highest bid for the inventory.

22 637. That is, publishers could send a standardized header to several exchanges, which included
23 information about the advertising slot and the visiting user, and bidders on the exchanges could within
24 milliseconds place bids for that advertising slot.

25 638. The new header-bidding technology threatened to cut Google out of the picture. Not only
26 did header bidding undermine Google's ad server, which had routed advertisements to the exchanges, it
27
28

FILED UNDER SEAL

1 also eroded Google's ability to front-run third-party ad exchanges by giving its own ad exchange an
2 information advantage.

3 639. Google created its own alternative to header bidding, called Open Bidding, which among
4 other things, allowed Google an advantage over other exchanges, including by charging a penalty fee
5 when an ad was sold on a non-Google exchange.

6 640. Google aggressively sought to quell the threat of header bidding, but the threat became
7 existential when Facebook threatened to adopt header bidding. In March 2017, Facebook publicly
8 announced it would support header bidding, including in connection with FAN. At that time, when
9 bidding into Google's ad server, networks such as Facebook's FAN had to bid into exchanges and pay
10 exchange fees. By adopting header bidding, Facebook would let web publishers, mobile app publishers,
11 and advertisers avoid Google's exchange fees altogether. They could simply header bid to the exchanges,
12 including through Facebook's valuable FAN.

13 641. This was viewed as a direct attack on Google's supremacy. Ad Age reported as much on
14 March 22, 2017:

15 Facebook just executed what might best be described as a digital
16 advertising coup against rival Google and its DoubleClick empire.

17 The social media power said Wednesday that it's bringing advertiser
18 demand from its Audience Network to mobile web publishers that use
header bidding.

19 Mobile publishers have been able to tap demand from Facebook Audience
20 Network until now so long as they didn't use header bidding technology, a
21 system that allows them to take bids from multiple buyer pools all at once.
But if they wanted to capitalize on header bidding, they had to forgo any
demand in FAN.

22 Now publishers that used header bidding and want to tap advertisers
23 coming through FAN can do so through Facebook technology partners
24 Index Exchange, Sonobi, Amazon Publisher Services, AppNexus,
Media.net and Sortable. They can also access FAN through open-source
25 solutions PreBid and PubFood, the company said.

26 642. As Ad Age observed, the move meant that Facebook's preeminent, identity-based
27 targeting system could now be leveraged across the internet:

FILED UNDER SEAL

Publishers like the Washington Post, Daily Mail and Forbes have been quietly working with Facebook to introduce the offering, which gives them the ability to plug into FAN and receive ads bought through Facebook's sophisticated data and targeting technology.

643. Facebook's move had been part of a long-term strategy to draw in Google. Facebook's gambit worked, and Google reached out to Facebook to broker a deal.

D. Google Agrees to Help Facebook Identify Facebook's Own Users Outside of Its Walled Garden, and Facebook Backs Off of Programmatic and Exchange-Trade Advertising

644. Within months of Facebook's official header bidding announcement, Google and Facebook began formal negotiations. By August 2018, the companies were in heated negotiations, with each company internally evaluating contingencies and strategies if no deal could be reached.

645. In September 2018, the companies finally reached an agreement—an anticompetitive one. The agreement was code-named Jedi Blue.

646. Facebook agreed to back off its support of header bidding, leaving Google's dominant position over exchange-based advertising intact.

647. In exchange, Google agreed to give Facebook what it needed—a means to track its own users when outside of Facebook-controlled apps.

648. As part of the agreement, Facebook would pay Google a 5 to 10% transaction fee and would be locked into spending \$500 million annually on Google's exchange-based systems.

649. Facebook, in return, would keep its control over the Social Advertising Market. In fact, because of the agreement, Facebook was able to ensure that Google's targeting would not target Facebook's users, solidifying Facebook's preeminence over advertising to users on its social networks. In short, Facebook's agreement with Google shored up Facebook's DTBE within its walled garden at a time when the very existence of a differentiated, Facebook-dominated Social Advertising Market was under threat from advancements in programmatic advertising and tracking technology.

650. As reported by the *Wall Street Journal*, Google provided Facebook a series of concessions to Facebook as part of Jedi Blue that ensured this. For example:

FILED UNDER SEAL

- Google would help Facebook recognize mobile and web users, particularly Facebook’s own users as they used websites and third-party applications.
- Facebook would receive the right to show ads to 90% of the users it recognized as its own.
- Facebook would receive a 300 millisecond “timeout” to recognize its users and bid. Other participants would receive a shorter, 160 millisecond timeout.

651. The threat of Facebook leveraging its targeting systems in Google’s space was quelled—by agreement. In exchange, Google propped up the Social Advertising Market. Because Facebook could identify its own users outside of its apps, Facebook could maintain a price premium when it sold advertisements to those users. Facebook also received preference over those users, meaning bidders on other exchanges would only get the remaining 10% of inventory, and even then, would have half the time Facebook had to bid on that inventory.

652. Google handed Facebook control over advertising targeting Facebook users and users of other Facebook-controlled apps. This meant that Facebook became the most valuable means of reaching these users, including while using third-party apps or websites.

653. Without the agreement, Google’s machine-learning and AI dominance would allow it to identify users, including Facebook’s own users, and target them, eventually based on granular criteria. This would erode the DTBE protecting Facebook’s Social Advertising Market and reduce the price premium Facebook could charge (and did charge) for reaching its users.

654. Because of Jedi Blue, Facebook’s users remained uniquely Facebook’s to advertise to. As a result, advertisers had to pay Facebook (at a premium) to advertise to those users using granular targeting, including demographic-based targeting. By reason of the Jedi Blue agreement, no fungible level of targeted advertising could (or did) emerge that could rival Facebook’s ad products for its walled garden users.

655. The agreement also neutralized (or at least substantially delayed) the AI and machine-learning threat posed by Google. Although Google was able to determine the identity of users based on publisher-provided information and its own data collected throughout the Internet, it would not leverage that data to poach advertising sales from Facebook. Rather, Facebook would receive priority over

FILED UNDER SEAL

1 advertisements to its own identified users—and would receive Google’s help to identify those users.
2 Instead of turning its technology against Facebook, Google used it to bolster Facebook’s dominant
3 position in the Social Advertising Market.

4 656. Put simply, Google and Facebook agreed to divide and segment markets, allowing
5 Facebook to continue charging a significant price premium for its targeted advertising sold in the Social
6 Advertising Market. The agreement also staved off competition that threatened Google’s control over
7 exchange-traded advertising throughout the Internet. Both competitors benefited. Competition did not.

8 **XI. FACEBOOK ANTICOMPETITIVELY INTEGRATES THE BACKENDS OF**
9 **INSTAGRAM, WHATSAPP, MESSENGER, AND ITS CORE FACEBOOK PRODUCT**

10 657. Facebook had entered into an agreement with Google to identify Facebook users as they
11 interacted with websites and apps outside of Facebook’s walled garden. With its resources freed up,
12 Facebook turned inward to finally seal off any competition in the Social Advertising Market, significantly
13 and irreversibly strengthening the DTBE.

14 658. Facebook had for years operated its WhatsApp and Instagram applications as separate
15 businesses. Indeed, Facebook pledged to regulators to keep the companies and their massive data stores
16 separate. [REDACTED]

17 [REDACTED]
18 [REDACTED]
19 [REDACTED] The purpose of this integration was not (legitimately) technical; rather, the entire plan was an
20 attempt to irreversibly commingle Facebook’s various data sources, products, and models so that
21 regulators could not eventually break up, divest, or otherwise cleanly enjoin or monitor the company after
22 a year of growing, worldwide concern about Facebook’s data practices and market power.

23 659. [REDACTED] By
24 March 2019—[REDACTED]
25 [REDACTED]
26 [REDACTED]—numerous U.S. Senators, including Presidential candidate Elizabeth Warren, had
27 expressly and publicly called for the company to be broken up.
28

FILED UNDER SEAL

1 [REDACTED] Zuckerberg and Facebook [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]

15 662. Facebook's back-end integration lacked any legitimate technical justification, but was
16 instead solely a means to prevent the regulatory breakup of Facebook, Instagram, and WhatsApp and to
17 cement Facebook's dominance over the Social Advertising Market.

18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24
25
26
27
28

FILED UNDER SEAL

1

2

3

4

[REDACTED]

15

16

17

18

19

20

21

22

23

24

25

26

27

28

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11

[REDACTED]

[REDACTED]

25
26
27
28

[REDACTED]

FILED UNDER SEAL

1

2

3

4

5

6

7

8

9

10

23

24

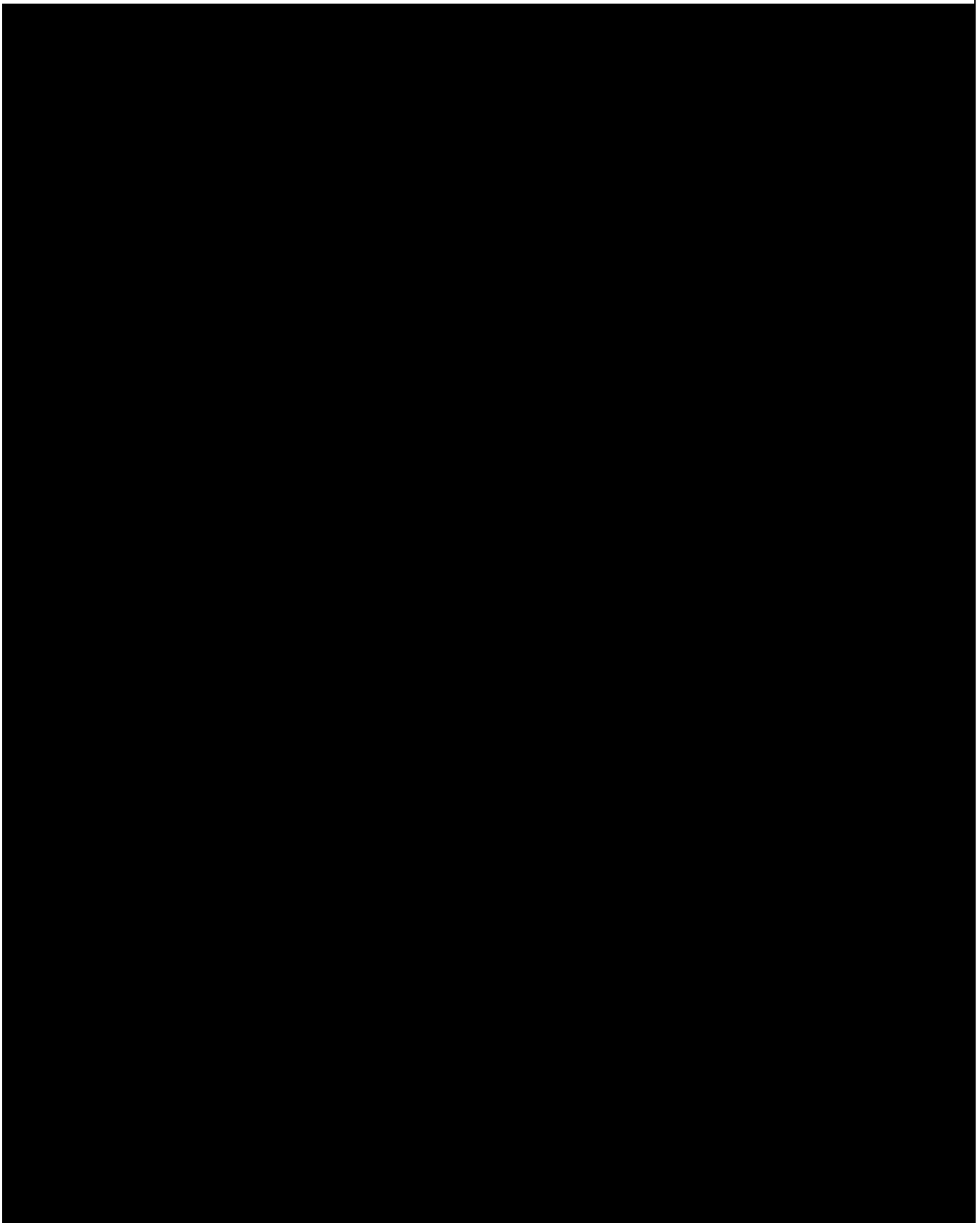
25

26

27

28

FILED UNDER SEAL



FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FILED UNDER SEAL

1

2

[REDACTED]

14

15

16

17

18

19

20

21

22

23

24

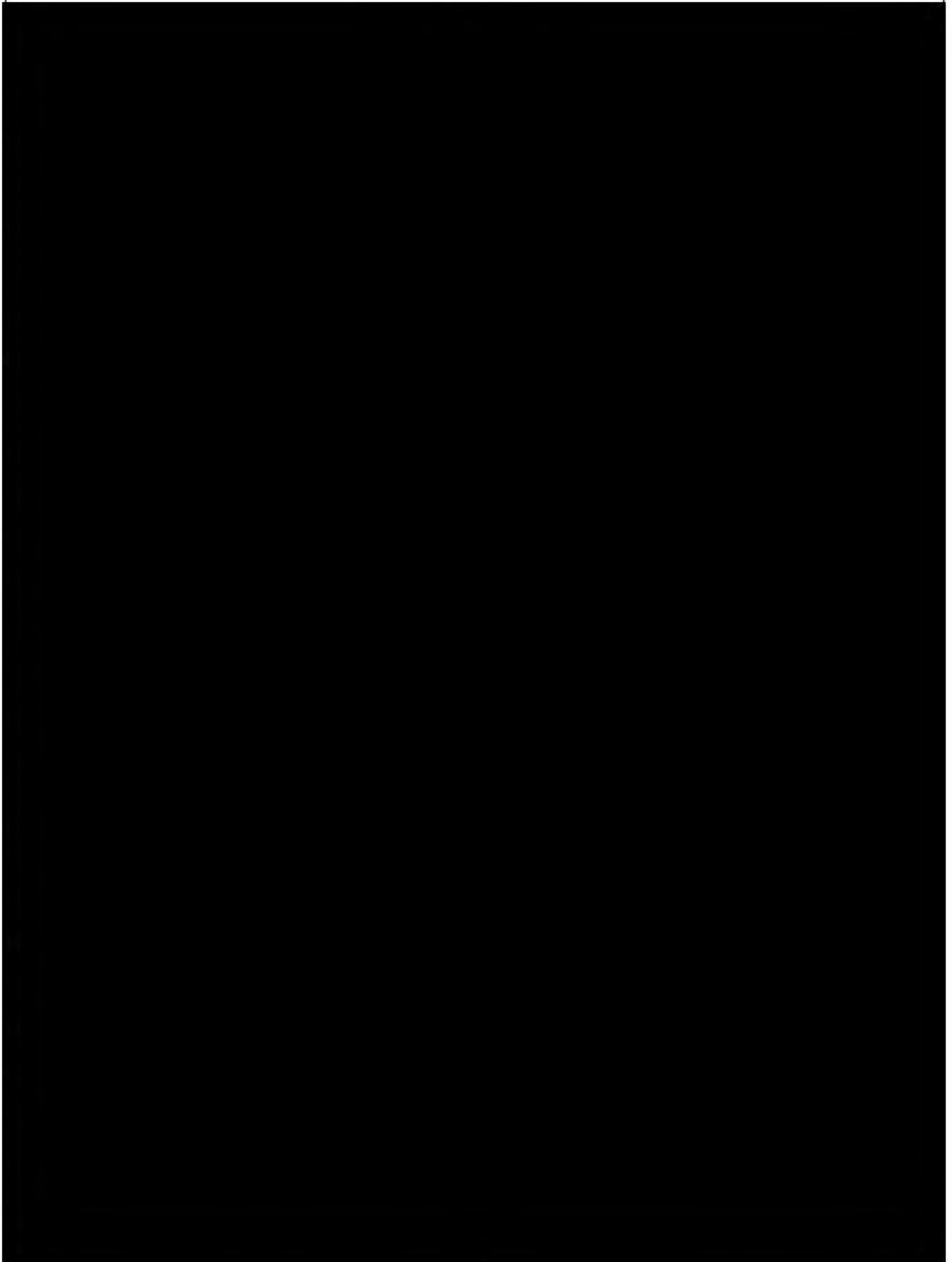
25

26

27

28

FILED UNDER SEAL



[illegible]

FILED UNDER SEAL

690. At the time of the Instagram and WhatsApp acquisitions, Facebook had promised regulators that it would operate Instagram and WhatsApp as separate businesses from its core applications, Facebook and Messenger.

691. For example, Facebook had represented to the European Commission's competition regulator that it was unable to match user profiles across WhatsApp and Instagram. The EC regulator relied on those statements as part of its 2014 merger review process.

692. On May 17, 2017, the EC regulator fined Facebook €110 million and explained its reasons for the fine in the following press release:

The European Commission has fined Facebook €110 million for providing incorrect or misleading information during the Commission's 2014 investigation under the EU Merger Regulation of Facebook's acquisition of WhatsApp

When Facebook noticed the acquisition of WhatsApp in 2014, it informed the Commission that it would be unable to establish reliable automated matching between Facebook's users' accounts and WhatsApp users' accounts. It stated this both in the notification form and in a reply to a request for information from the Commission. However, in August 2016, WhatsApp announced updates to its terms of service and privacy policy, including the possibility of linking WhatsApp users' phone numbers with Facebook users' identities.

On December 2016, the Commission addressed a Statement of Objections to Facebook detailing its concerns.

The commission has found that, contrary to Facebook's statements in the 2014 merger review process, the technical possibility of automatically matching Facebook and WhatsApp users' identities already existed in 2014, and that Facebook staff were aware of such a possibility.

FILED UNDER SEAL

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] In March 2018, WhatsApp's founder Brian Acton quit in protest, stating on Twitter: "It is time. #deletefacebook."



697. Zuckerberg had reneged on his promise to limit the monetization of WhatsApp for five years, and had almost immediately begun to monetize WhatsApp by matching WhatsApp's massive user base with Facebook's existing user profiles in order to target advertising and to collect social data.

698. Acton left behind \$850 million in stock when he quit in protest.

699. WhatsApp's other co-founder, Jan Koum, left in April of 2018. Likewise, Instagram's founders Kevin Systrom and Mike Krieger followed suit shortly after, resigning from Facebook in the Fall of 2018.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FILED UNDER SEAL**D. The Call to Break Up Facebook, WhatsApp, and Instagram**

701. On March 20, 2018, the Washington Post reported that the Federal Trade Commission had opened an investigation after Facebook's infamous Cambridge Analytica scandal. In the run-up to the 2016 United States Presidential election, Facebook had allowed Cambridge Analytica to pull massive amounts of user information through Facebook's APIs, affecting tens of millions of Facebook's users. The scandal was surprising, as Facebook had been telling developers and the public that it was no longer allowing third-party apps to access to a user's friends and feed information. The FTC immediately began looking into whether Facebook had violated its 2011 consent decree with the agency.

702. On April 10, 2018, Mark Zuckerberg was called to testify before the United States Senate. Senators' questions pointedly turned to Facebook's monopoly position, particularly during questioning by Senator Lindsey Graham of South Carolina. Graham repeatedly questioned Zuckerberg about Facebook's competitors, and directly asked him if the company had a monopoly.

703. By the end of 2018, there was widespread public sentiment, including in Washington D.C., that Facebook had become an anticompetitive monopolist. Several United States Senators introduced measures to reduce Facebook's market power, including by proposing modifications to statutory provisions under the Communications Decency Act that have been interpreted to provide Facebook with broad legal immunities that many other companies did not and do not enjoy. As a September 5, 2018, article in The Verge recounted:

In some ways, Facebook is the most urgent case. It's inescapable, opaque, and wields immense power over the fundamental functions of our society. More than any other tech giant, Facebook's power feels like an immediate threat and the most plausible first target for congressional action. Sen. Mark Warner (D-VA) has already laid out 20 different measures that would rein in Facebook and other tech giants, ranging from GDPR-style data portability requirements to more carveouts of Section 230.

But while Warner's measures focus on nudging Facebook toward more responsible behavior, a growing number of critics see the problem as Facebook itself. It may be that a social network with more than 2 billion users is simply too big to be managed responsibly, and no amount of moderators or regulators will be able to meaningfully rein the company in. For those critics, social networks are a natural monopoly, and no amount

FILED UNDER SEAL

1 of portability requirements will ever produce a meaningful competitor to
2 Facebook or a meaningful check on its power.

3 If that's true, *a classical antitrust breakup (as some have suggested)*
4 *would seem like the only option.*

(emphasis added).

5 704. Cries to break up Facebook were becoming more common. Professor Tim Wu, known for
6 his work on “net neutrality”—in fact, for coining the phrase—had called for Facebook’s breakup. His
7 focus was Instagram and WhatsApp. A September 2018 article in The Verge explained Wu’s position:

8 I think if you took a hard look at the acquisition of WhatsApp and
9 Instagram, the argument that the effects of those acquisitions have been
10 anticompetitive would be easy to prove for a number of reasons, says Wu.
And breaking up the company wouldn’t be hard, he says.

11 705. On March 8, 2019, Senator Elizabeth Warren—then running for President of the United
12 States—directly called for the breakup of Facebook. Warren’s focus was on the Instagram and WhatsApp
13 acquisitions. As Warren stated in a blog post, she believed several big tech mergers should be unwound,
14 including Facebook’s WhatsApp and Instagram acquisitions:

15 Current antitrust laws empower federal regulators to break up mergers that
16 reduce competition. I will appoint regulators who are committed to using
existing tools to unwind anti-competitive mergers, including:

- 17 ▪ Amazon: Whole Foods; Zappos
- 18 ▪ Facebook: WhatsApp; Instagram
- 19 ▪ Google: Waze; Nest; DoubleClick

20 Unwinding these mergers will promote healthy competition in the
21 market—which will put pressure on big tech companies to be more
responsive to user concerns, including about privacy.

22 [REDACTED]

23 [REDACTED]

24 [REDACTED]

25 [REDACTED]

26 [REDACTED]

[illegible]

reported on April 5, 2016, citing WhatsApp's own company blog—

SAN FRANCISCO – WhatsApp, the messaging app owned by Facebook and used by more than one billion people, on Tuesday introduced full

FILED UNDER SEAL

1 encryption for its service, a way to ensure that only the sender and recipient
2 can read messages sent using the app.

3 Known as “end-to-end encryption,” it will be applied to photos, videos, and
4 group text messages sent among people in more than 50 languages across
5 the world”

6 715. In short, Facebook had long already possessed the technology, the know-how, the
7 resources, and indeed the business experience to introduce end-to-end encryption in any of its other
8 messaging services, and to its photo, video, and group text functions across its various products. Indeed,
9 *Facebook had already done so in 2016, with WhatsApp.*

10 716. Moreover, encryption was, simply, a completely separate technical issue from integration.
11 Encrypting communications would not “integrate” anything (indeed, Facebook had chosen to end-to-end
12 encrypt WhatsApp, and nothing else, in 2016); and integrating multiple products would not suddenly
13 encrypt anything. The two technical concepts were—indisputably—totally distinct, [REDACTED]

14 717. However, using the phrase “end-to-end encryption” in any context did always bring one
15 predictable result: it immediately distracted from and overwhelmed any other technical issue in the
16 conversation, as law enforcement and civil libertarians would immediately fill the room with competing
17 views of electronic privacy at the mere mention of E2EE. The April 2016 New York Times article
18 announcing WhatsApp’s new end-to-end encryption was a case in point:

19 The move thrusts WhatsApp further into a standoff between tech
20 companies and law enforcement officials over access to digital data, one
21 that pits Silicon Valley’s civil libertarian ideals against the federal
22 government’s concerns over national security. Increased encryption will
23 make it more difficult, if not impossible, for the authorities to intercept
24 WhatsApp communications for investigations. . . .

25 End-to-end encryption for WhatsApp is of particular concern to the F.B.I.,
26 considering the service’s huge subscriber base and large international
27 footprint. With increasing amounts of communications now sent across
28 messaging services, encrypted texts, video, photos and the like may end up
being more problematic for law enforcement than locked devices. The
encryption on WhatsApp will be turned on by default, so users will not be
required to enable it themselves.

FILED UNDER SEAL

1 [REDACTED] So when Facebook's back-end integration—a completely distinct technical concept that
2 would irreversibly commingle the data and architecture of four different Facebook products to prevent
3 divestiture—was about to be thrust into the spotlight by Elizabeth Warren in March 2019, [REDACTED]

4 [REDACTED]

5 [REDACTED]

6 [REDACTED]
7 [REDACTED]

8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]

12 [REDACTED]
13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 721. And virtually every news outlet reported near-exclusively on the propriety and
19 background of end-to-end encryption and what it would mean for Facebook's products.

20 722. Congress and the U.S. Department of Justice also focused almost exclusively on
21 Facebook's announcements about end-to-end encryption. As Engadget reported on October 3, 2019:

22 The Department of Justice is set to ask Facebook to pause plans for end-
23 to-end encryption across all of its messaging services. It will urge the
24 company not to move forward "without ensuring that there is no reduction
to user safety."

25 Attorney General William Barr is set to make the request in an open letter
26 to Facebook CEO Mark Zuckerberg on Friday. Acting Homeland Security
27 Secretary Kevin McAleenan, UK Home Secretary Priti Patel and
28 Australian Minister for Home Affairs Peter Dutton also signed the draft
letter . . .

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

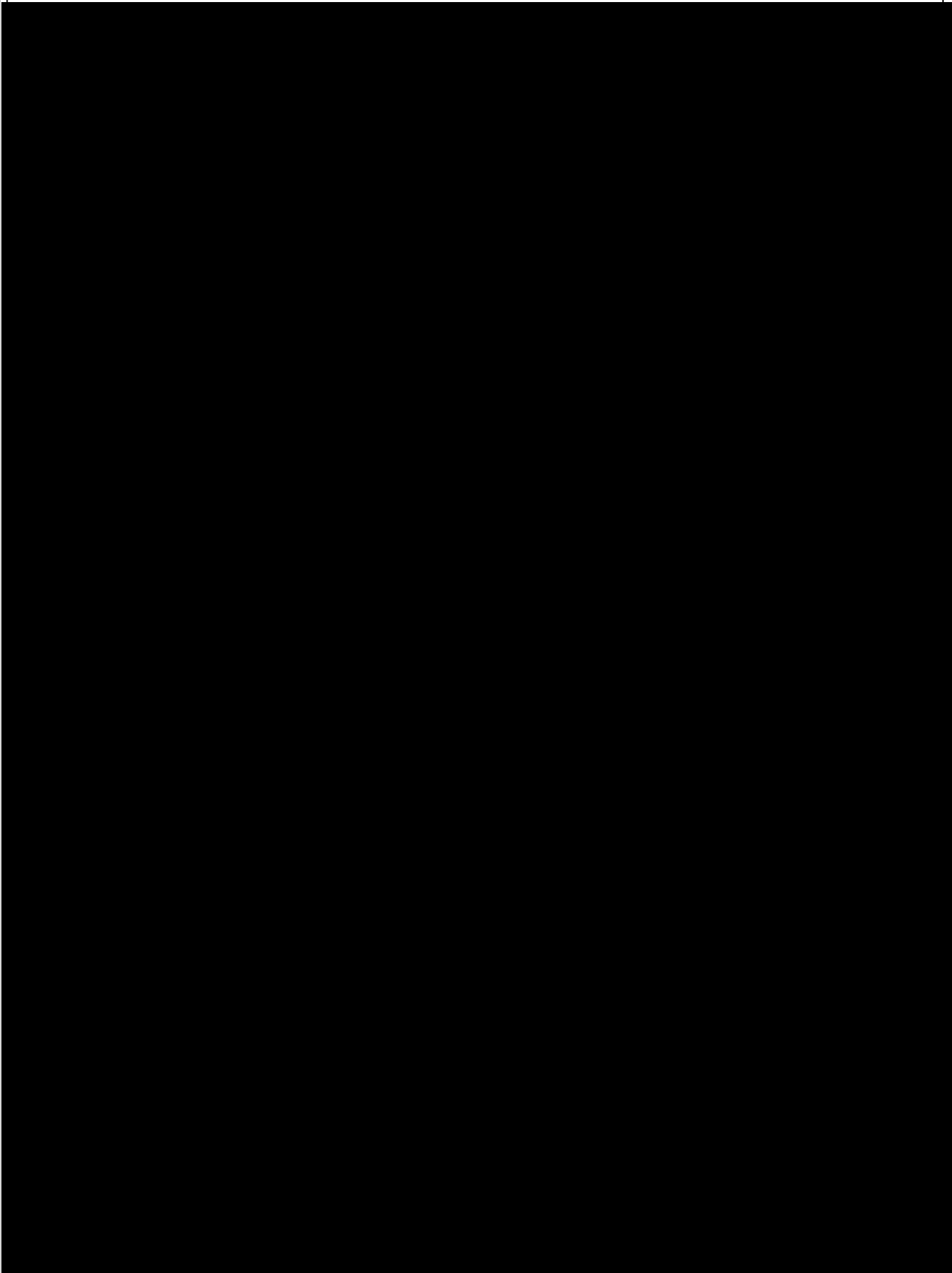
First Amended Consolidated Advertiser Class Action Complaint – Case No. 20-CV-08570-JD

FILED UNDER SEAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



First Amended Consolidated Advertiser Class Action Complaint – Case No. 20-CV-08570-JD

FILED UNDER SEAL

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED] And, likewise, end-to-end encryption could have been implemented at the application
5 level without integrating the back-ends of the messaging systems [REDACTED]
6 [REDACTED]

7 755. In fact, WhatsApp already had end-to-end encryption features as part of its messaging
8 Platform. As the WhatsApp website stated in April 2016:

9 Security by Default

10 WhatsApp's end-to-end encryption is available when you and the people
11 you message use the latest versions of our app. Many messaging apps only
12 encrypt messages between you and them, but WhatsApp's end-to-end
13 encryption ensures only you and the person you're communicating with
14 can read what is sent, and nobody in between, not even WhatsApp. This is
15 because your messages are secured with a lock, and only the recipient and
16 you have the special key needed to unlock and read them. For added
17 protection, every message you send has its own unique lock and key. All
18 of this happens automatically: no need to turn on settings or set up special
19 secret chats to secure your messages.

20 756. Again, WhatsApp posted about this on its company blog. The New York Times wrote an
21 article about it. Facebook knew how to implement end-to-end encryption within its products—and it had
22 already done it, years prior.

23 757. Indeed, WhatsApp had implemented end-to-end encryption in 2016, and nothing about
24 that feature required any form of integration with Instagram or Facebook Messenger. The purported
25 addition of “end-to-end encryption” in 2019 was not, as Facebook suggested, part and parcel with the
26 back-end integration. To the contrary, it had nothing to do with it.
27 [REDACTED]
28 [REDACTED]

FILED UNDER SEAL

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]

13 762. At the same time, these Facebook product changes that occurred in early 2019 and
14 continue (as far as Plaintiffs can discern based on limited discovery) to this day unquestionably
15 strengthened and fortified the DTBE and helped to maintain Facebook's dominance in the Social
16 Advertising Market, irreversibly bringing together massive quantities of social data [REDACTED]
17 [REDACTED] by Facebook.

18 763. Facebook's integration-related product changes had an anticompetitive effect in the Social
19 Advertising Market because, among other things, these product [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED] (i) by creating the largest aggregation of social targeting data the world has ever known, and (ii) by
23 preventing or substantially limiting the divestiture or separation (including court-ordered divestiture
24 pursuant to regulatory decree—and the Federal Trade Commission is currently seeking just this) of
25 discrete social data from WhatsApp, Instagram, and Facebook / Messenger.

26 764. But the above was an intended feature, not a bug. As explained in the previous sections,
27 these anticompetitive product changes by Facebook beginning in 2019 [REDACTED]
28

FILED UNDER SEAL

Moreover, as explained in the previous sections, these anticompetitive product changes lacked a legitimate technical (or non-anticompetitive) justification.

XII. THE RELEVANT MARKET

765. Plaintiffs are consumers and purchasers in the relevant market at issue in this case—the Social Advertising Market. Plaintiffs are direct purchasers of advertising products from Facebook and were anticompetitively harmed as participants in the Social Advertising Market.

A. The Social Advertising Market

766. The Social Advertising Market is a submarket of online advertising, the latter of which includes banner ads, search-based ads, and advertising on social networks. Social advertising, however, is not fungible or interchangeable with these other forms of online advertising. Indeed, social advertising allows advertisers to granularly target groups of users for ads by their attributes, including by the attributes of their networks.

767. Thus, because of the extensive ability to target advertisements to users on social media sites like Facebook, search and banner advertising are not reasonable substitutes.

768. Several relevant factors indicate that the Social Advertising Market is a distinct submarket of online advertising and more general advertising markets:

769. *Industry or public recognition of the submarket as a separate economic entity.* Social advertising is broadly considered to be distinct from other forms of advertising by market and industry participants. For example, the advertising company Outbrain describes the differences between social ads on its blog as follows:

Paid social ads are served via algorithms that define what the user might be interested in, based on past activity in their social accounts, such as likes, shares, and comments. Unlike search, which is a focused, goal-oriented activity, browsing on social is more relaxed. Think cat memes, vacation snaps, and fun quizzes. Nevertheless, the social platform has accumulated masses of data about every specific user, which can be leveraged to target specific audiences with ads that are likely to be of interest to them.

FILED UNDER SEAL

1 770. Outbrain explains that social ads are considered useful for a distinct purpose:

2 Social ads are best for targeting audience segments who may be interested
3 in your product or services, based on a range of targeting criteria—location,
4 age group, gender, hobbies, interests. Social networks, such as Facebook,
5 have advanced targeting capabilities, which means you can fine-tune your
6 targeting criteria to reach a very specific, high-quality audience.

7 771. Outbrain explains that search ads are different, as they “are great for targeting customers
8 when they are already looking for you (*i.e.*, they search your company name or product), or if they are
9 searching for a specific product, service, or piece of information that you can provide.” Outbrain also
10 distinguishes social advertising from other forms of online advertising, like discovery advertising.

11 772. Moreover, providers of business statistics such as statista.com also provide information as
12 to social media advertising as a distinct submarket of online and general advertising.

13 773. As another example, in March 2015, leading advertising publication AdAge referred to
14 Facebook’s Custom Audience targeting, which is unique to social advertising, as “potentially different
15 and more special because they have this richer level of data.”

16 774. Likewise, industry publication Marketing Land reported in an October 14, 2019 article
17 that media agency Zenith, which is owned by Publicis Media, predicted growth in the social media
18 advertising segment as distinguished from search and television advertising, with social media ads
19 coming in third behind television and paid search advertising.

20 775. On an October 23, 2012 earnings call, Facebook’s COO Sheryl Sandberg said, “On the
21 question of where advertisers are, as I’ve said before, we are a third [thing]. We’re not TV, we’re not
22 search. We are social advertising, and I would say our clients are on different parts of that adoption
23 curve.” Later, on a May 1, 2013 earnings call, Sandberg explained: “As I said before, the thing about
24 brand advertisers is that they got very used to TV, then they got very used to search, and we are a third
25 thing.”

26 776. Even academic articles, including those published in the Journal of Advertising, have
27 analyzed the market for social media advertising as a distinct segment, with well-defined engagement
28 characteristics.

FILED UNDER SEAL

1 777. *The product's peculiar characteristics and uses.* Social advertising has a distinct purpose
2 from other forms of advertising. Social advertising has different applications than other forms of online
3 advertising. Namely, social advertising allows granular targeting based on user attributes, user interests,
4 and group attributes. Moreover, because of the detailed amount of information that can be collected about
5 users as they engage on social media platforms, social advertising can seek out other users with similar
6 behavioral characteristics.

7 778. Facebook, for example, describes its own targeting capabilities as follows:

8 Facebook ads can be targeted to people by location, age, gender, interests,
9 demographics, behavior and connections. You can also use more advanced
10 targeting tools like Lookalike Audiences, which lets you target people
11 similar to the people who already engage with your business, or you can
12 layer your targeting options to select a more specific audience.

13 779. Facebook allows advertisers to create Lookalike audiences. Thus, unlike search or other
14 forms of advertising where the ad is created and placed to reach a preexisting audience, Facebook is able
15 to algorithmically combine a subset of its users to fit an advertisement. This capability is unique to social
16 advertising.

17 780. As Facebook explains on its website:

18 When you create a Lookalike Audience, you choose a source audience (a
19 Custom Audience created with information pulled from your pixel, mobile
20 app, or fans of your page). We identify the common qualities of the people
21 in it (for example, demographic information or interests). Then we deliver
22 your ad to an audience of people who are similar to (or “look like”) them.

23 781. Because of the level of granular data Facebook collects from its users, it can provide
24 targeting flexibility like no other advertising medium. As Facebook explains:

25 You can choose the size of a Lookalike Audience during the creation
26 process. Smaller audiences more closely match your source audience.
27 Creating a larger audience increases your potential reach, but reduces the
28 level of similarity between the Lookalike Audience and source audience.
We generally recommend a source audience with between 1,000 to 50,000
people. Source quality matters too. For example, if a source audience is
made up of your best customers rather than all your customers, that could
lead to better results.

FILED UNDER SEAL

782. Social advertising is also marked by the ability to algorithmically refine advertising targeting as users interact with the ads. For example, Facebook allows users to place a pixel on their website that is pulled off Facebook's servers when the site is accessed. Facebook is thus able to determine the efficacy of ads run on Facebook once the user transitions to an advertiser's own website. Over time, Facebook's advertising becomes more targeted and more effective in terms of particular advertising goals, such as lead generation or online purchases.

783. Other social networks, such as Twitter, provide similar targeting abilities. Twitter, for example, allows targeting based on location, language, device, age, and gender, but also allows for the targeting of audience types, including algorithmically tailored and custom-created audiences.

784. These targeting features, which are available on social advertising platforms, are not comparably available as part of other forms of online advertising, such as display and banner ads or search ads.

785. ***Unique production facilities.*** Social advertising requires data collected from users on an inherently social application. A user's search history, for example, will not provide enough data to create highly targeted advertising features, such as Facebook's Lookalike Audiences. Likewise, passive advertising, such as banner ads, or even general magazine or publication ads, provides little granular data that can then be used to further refine the targeting of advertising.

786. Providers of social advertising require specialized means of production because they must rely on data harvested from engagement among networks of users to facilitate highly targeted advertising. Platforms capable of delivering social advertising must therefore provide functionality such as image and video sharing, messaging, matchmaking, content sharing, and other inherently social features in order to obtain the data needed to allow for granular user and user network targeting.

787. Because social advertising allows iterative refinement of target audiences, a provider of social advertising must employ machine-learning or artificial intelligence algorithms that are trained on data collected from users as they interact and engage with content and advertising. As Facebook's head of its Applied Machine Learning Group, Joaquin Quiñonero Candela, told *Wired* magazine (emphasis in original):

FILED UNDER SEAL

1 **Facebook today cannot exist without AI.** Every time you use Facebook or
2 Instagram or Messenger, you may not realize it, but your experiences are
3 being powered by AI.

(emphasis added).

4 788. Other forms of advertising generally do not require sophisticated machine learning or
5 artificial intelligence. For years prior to the advent of modern machine learning techniques, search
6 engines such as Yahoo and Google used far less sophisticated algorithms to match user searches with
7 suggested websites and, in turn, advertisements. Traditional advertising, such as magazine or television
8 ads, require no algorithms at all, let alone artificial intelligence.

9 789. **Distinct customers.** Social advertising customers are distinct from search advertisers and
10 passive display advertisers. Moreover, social advertising is generally more effective at targeted
11 advertising rather than reaching a massive number of people.

12 790. Customers advertising on search engines are generally seeking priority among the search
13 results returned given a particular keyword. Customers advertising on social media platforms are
14 searching for users that fit a particular, predefined profile or set of characteristics. Small businesses that
15 do not generally have the budget to bid on coveted search results are nonetheless able to bid on granularly
16 defined audiences on a social media platform like Facebook.

17 791. **Distinct prices and sensitivity to price changes.** Social advertising prices are distinct from
18 other forms of advertising. In search-based advertising, certain search keywords are bid up by many
19 advertisers seeking to have their ads displayed as part of search results. This means that prices in certain
20 categories, such as legal or home improvement, will be significantly higher on search-based platforms
21 than on social advertising platforms like Facebook. For example, legal ads are on average \$1.32 on a
22 cost-per-click basis on Facebook, whereas they are \$6.75 on a cost-per-click basis on the Google Ads
23 platform. Likewise, consumer services ads are on average \$3.08 on a cost-per-click basis on Facebook's
24 platform vs. \$6.40 on Google Ads.

25 792. Because bidding on Google Ads and other search-based advertising is zero sum, meaning
26 only a certain number of ads can be coupled with a particular set of search keywords, pricing is more
27 sensitive to changes in demand.

FILED UNDER SEAL

793. Social advertising, however, allows granular targeting, avoiding much of the zero-sum nature of other forms of advertising bidding. Moreover, social advertisers like Facebook can tailor audiences, reducing the likelihood that advertisers will have to compete for the same display opportunity at any given point in time.

794. Other general forms of advertising such as television and print are even more zero-sum, as there are limited time slots or available pages in a newspaper or magazine. Pricing is thus more sensitive to demand in these forms of advertising.

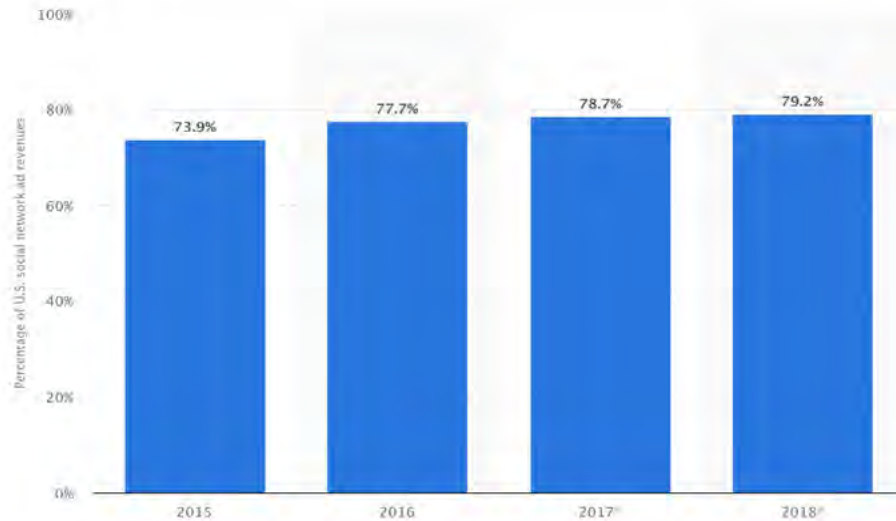
795. Social advertising is thus entirely distinct. Because of the ability to target audiences to advertising, pricing is proportional to the generality of the targeting, not simply to the general demand for a limited search term, key word, or periodical placement.

796. Moreover, Facebook has been able to consistently raise its prices in almost every year it has sold advertising without facing price pressures from competitors. On a cost per mille (CPM)—or cost per thousand advertising impressions—basis, Facebook’s advertising prices grew 90 percent year over year according to a report at the end of 2019. In 2018, Vox reported that CPM prices on Facebook had increased 122 percent year over year. In 2017, Facebook’s CPMs increased 171%. Facebook raised prices in prior years as well.

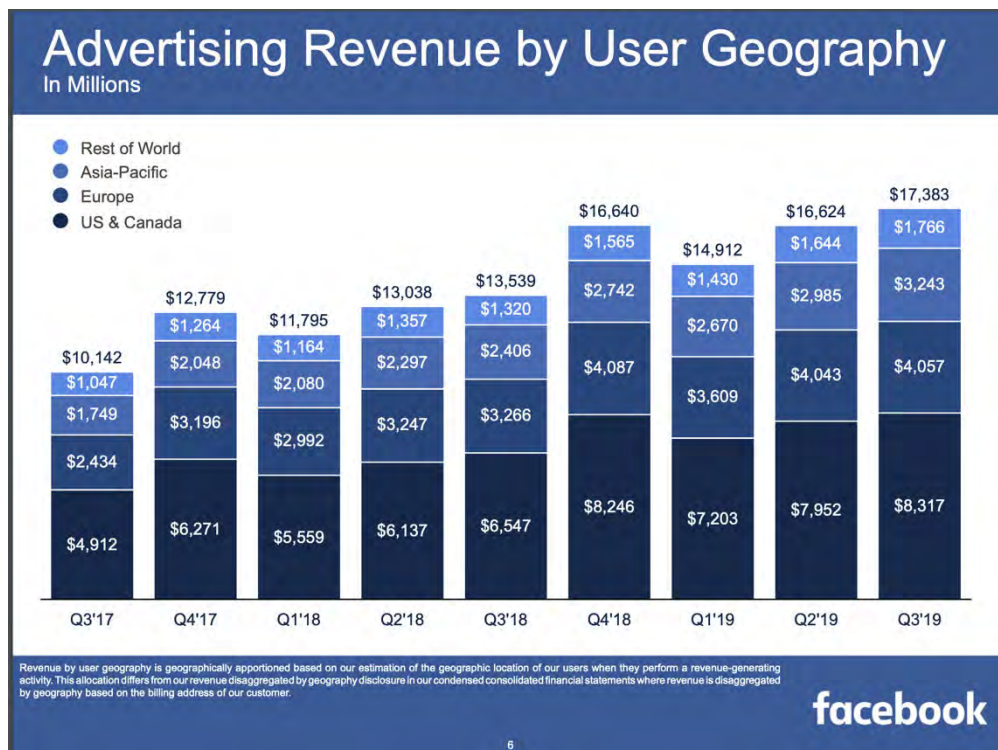
797. ***Specialized vendors.*** The Social Advertising Market has its own distinct and specialized vendors, namely advertising agencies such as Lyfe, Thrive, Volume Nine, Sociallyin, and Firebelly Marketing, all of which boast a specialization in social media advertising and provide specialized social media management products. There are many such specialty advertising agencies that specialize in creating social media advertising campaigns. Moreover, specialized social media analytics vendors also exist, such as Socialbakers, which provides aggregated analytics across social media platforms. There is an entire ecosystem of vendors specializing in social advertising—an indicator that the Social Advertising Market is its own distinct submarket of online advertising, requiring its own unique tools and expertise.

FILED UNDER SEAL

798. Facebook's revenue share of the Social Advertising Market is approximately 80%. Its share has been above 70% since 2015. It remains above that threshold to this day.



799. Facebook's advertising revenue has steadily grown both in the United States and globally. Facebook reported advertising revenues totaling \$17.383 billion as of Q3 2019. Approximately \$8.3 billion of that advertising revenue came from the United States.



FILED UNDER SEAL

800. From 2014 to 2016, Facebook's advertising revenues grew from \$2.9 billion to \$6.436 billion. During that period, and even before then, Facebook was one of the few social networks that significantly monetized its network by selling advertising. Other competitors did not come close, and Facebook established unrivaled dominance in the Social Advertising Market and maintains that dominance to this day.

801. Twitter, one of Facebook's only competitors to sell significant social advertising during the same period Facebook generated revenue in the Social Advertising Market, has never exceeded \$800 million in advertising revenues. Revenues in Q1 2012 were approximately \$45 million, growing to \$432 million in Q4 2014, and standing at \$702 million as of Q3 2019.

802. LinkedIn, another competitor that sells social advertising, generated roughly \$2 billion in overall annual revenue by the end of 2018, with some portion of that coming from advertising.

803. Considering the revenue generated by LinkedIn and Twitter, Facebook's advertising revenue accounts for approximately 86% of the total revenue share across the three largest firms competing in the Social Advertising Market. Excluding the contributions from minor competitors that monetize their social networks, the HHI of the Social Advertising Market is approximately 7,685, well beyond what the DOJ considers a highly concentrated market.

B. Barriers to Entry

804. The Social Advertising Market is protected by the Data Targeting Barrier to Entry that prevents Facebook's competitors from entering the market. Without a critical mass of social data and machine-learning / AI technology, market participants in the Social Advertising Market cannot generate revenue.

805. Moreover, without adequate social data and engagement with the social network, market participants cannot display content to users that would provide enough value to generate engagement and additional social data.

806. Likewise, without a critical mass of social data, advertising targeting will not be possible or will be substantially diminished in effectiveness, thus reducing revenues in the advertising sales in the Social Advertising Market.

FILED UNDER SEAL

807. A firm's market power in this market therefore depends on obtaining a critical mass of social data and the technology to mine it. Because of network effects, users will not use a social network that lacks enough social data to provide targeted content or to provide valuable connections to other users. However, once a certain amount of social data is obtained by a market participant, a feedback loop may form as a result of network effects, further increasing the amount of social data generated by the social network.

808. A new entrant must therefore expend significant amounts of investments in capital, technology and labor to create a network large enough to create the network effects necessary to compete with dominant firms in the market.

809. Because of the large amount of capital and social data required to successfully enter the Social Advertising Market, the DTBE effectively excludes entry by a new competitor, even a well-funded one. Indeed, the DTBE prevented Google from successfully entering the market for social data and the Social Advertising Market with its Google+ social networking product.

810. Although Google+ had successfully replicated Facebook's core functionality and even added additional functionality to its software, its entry failed because it lacked the critical mass of social data that is required to reverse the network effects protecting Facebook. Without that critical mass, users will not incur the costs of switching from Facebook's social network to a new entrant's social network. That is, a new entrant will not be able to provide a valuable network of engaged users upon entry to justify a Facebook user to change social networks.

811. That is precisely what happened to Google. Although it had a massive user base, it lacked engagement, which meant it did not provide a sufficient amount of social data that could be used to target content and advertising to users. This, in turn, reduced the value of the entrant social network and accordingly the attraction of switching from Facebook's social network to Google's.

812. The DTBE continues to reinforce Facebook's dominant position. In fact, by excluding rivals and potentially competing social networks through the anticompetitive scheme described in this Complaint, Facebook strengthened the DTBE, providing it a larger share of social data and a stronger

FILED UNDER SEAL

monetization channel through social advertising. The additional amount of social data increases the value of its network, and the revenue from social advertising increases the cost of entry for a new rival.

813. Other barriers to entry in the Social Advertising Market include, but are not limited to, the high cost of development, data management, talent acquisition and retention, server infrastructure, development infrastructure, software technology, software libraries, and a brand and marketing presence sufficient enough to attract an engaged user base.

C. Relevant Geographic Market

814. The relevant geographic market is the United States Social Advertising Market.

815. For the social data that fuels a social advertising product, social data must be compatible with the customers purchasing that data. Thus, social data about a foreign market may be of little use for a U.S.-based advertiser. The data may be collected in a different language, may involve interests more pertinent to a particular geographic region (*e.g.*, American Football vs. Rugby), and may contain a demographic of users that share a common culture or merely a close proximity.

816. The same is true for the Social Advertising Market. An advertiser seeking to sell products designed for consumption in the United States may not have any use for a platform's advertising targeting capabilities outside of the United States. In the U.S., Facebook enjoys a higher market share of the Social Advertising Market than it does worldwide (which is already very high, as described in subsection VI.A). In short, Facebook enjoys an even more dominant share of the U.S. Social Advertising Market than it does globally.

817. In the U.S., Facebook's market share of the social data generated by users is even greater than its global market share. Services such as WeChat are geared towards Asian markets, particularly China, and do not generally compete in the U.S. market with Facebook's Messenger, Instagram, and core social networking product. Thus, Facebook's U.S.-based market share is even higher than its global market share referenced above in VI.A, which is already a dominant share of the Social Advertising Market.

FILED UNDER SEAL**XIII. HARM TO COMPETITION AND ANTITRUST INJURY**

818. Facebook's anticompetitive scheme had the purpose and effect of monopolizing the Social Advertising Market in the United States. Facebook's conduct allowed it to maintain the monopoly and market power it had obtained by 2010 in the Social Advertising Market, and/or Facebook intended and attempted to acquire such a monopoly through its anticompetitive scheme.

819. Specifically, Facebook engaged in a series of acts in furtherance of its scheme, including, but not limited to:

- the targeting of competitors for coercive Whitelist and Data Sharing Agreements on pain of denial of access to Facebook's Platform and APIs, including Facebook's Events APIs;

- [REDACTED]
- [REDACTED]

- entering into an anticompetitive agreement with Google to bolster and reinforce Facebook's dominant position in the Social Advertising Market; and

- [REDACTED]

820. This conduct, each individually, and together as a whole, harmed competition in at least the following ways:

FILED UNDER SEAL

821. *First*, Facebook's conduct resulted in the exclusion of actual and potential competitors from the Social Advertising Market. By entering into a series of anticompetitive whitelist and data sharing agreements after scuttling its Platform, Facebook was able to obtain a superset of the social data collected by third-party apps. Facebook leveraged deprecation decisions, [REDACTED], to obtain social data and signals from third parties. [REDACTED]
[REDACTED]
[REDACTED]. Facebook fended off the threat beyond its walled garden with an anticompetitive agreement with Google. Facebook used deception to obtain through Onavo spyware user information that ordinary competitors would not have access to—
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. This conduct collectively ensured that a rival Social Advertising Platform could not enter the market and that regulators could not break up Facebook or otherwise regulate its conduct.

822. *Second*, Facebook's conduct reduced consumer choice / welfare. Facebook's conduct ensured that there would be no competition by a rival social advertising platform on non-price bases, such as, for example, increased privacy, more features, higher quality features, new features, more valuable social connections, reduced advertising to users, or new use cases. The scheme also foreclosed new or alternate business models by competitors or potential competitors.

823. Additionally, Facebook's Onavo surveillance system exfiltrated personal and sensitive data from user devices, [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. Moreover, this stolen

FILED UNDER SEAL

Onavo data was not available to rivals or potential entrants in the Social Advertising Market, ensuring that there would be no competitive price check to Facebook's supracompetitive social advertising prices.

824. Likewise, user data was incorporated into Facebook's advertising targeting systems by virtue of [REDACTED]. The net result was to strengthen Facebook's position in the Social Advertising Market, reducing the ability of other firms to enter the market, particularly without access to [REDACTED] Facebook obtained by threatening competition with, and capturing data from, these companies.

825. Facebook also reduced advertising consumer choice. Because of Facebook's conduct, Facebook's targeting ability vastly increased and the ability of a potential competitor to access a meaningfully unique store of social data was sealed off, preventing other social advertising companies from entering the Social Advertising Market. This resulted in fewer Social Advertising choices for advertisers and left only Facebook's monopoly rents as available prices in the Social Advertising Market.

826. *Third*, Facebook's conduct allowed it to raise prices. Facebook's anticompetitive scheme has allowed it to raise prices for social advertising during and the execution of the scheme and Facebook's course of conduct, including across both class periods. Facebook continues to be one of the only sources for targeted social advertising in the United States and in most of the world. As evidence of its market power in the Social Advertising Market, Facebook has raised prices without sacrificing any demand.

827. For example, Facebook's requirement that developers purchase advertising as a condition of maintaining access to Platform features artificially created demand for Facebook's advertising products, particularly its mobile advertising product. This had the purpose and effect of directly inflating advertising prices.

828. Similarly, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FILED UNDER SEAL

[REDACTED], and ultimately allowed Facebook to maintain and raise prices in the Social Advertising Market with little or no competitive check in the months and years [REDACTED].

829. In addition, Facebook's anticompetitive agreement with Google allowed Facebook to track Facebook, Instagram, and WhatsApp users outside of those applications and gave Facebook priority when advertising to them. As a result of that agreement, Facebook did not meaningfully compete with Google in programmatic and display-based advertising product markets and sub-markets, and Google did not leverage its ability to identify and target Facebook users, which would diminish Facebook's dominance over targeted advertising to those users while on Facebook's social network. Because Google bolstered and reinforced Facebook's dominant position and market power in the Social Advertising Market, Facebook was able to maintain and raise prices with little or no competitive check.

830. Next, by strengthening the DTBE, eliminating competition and preventing competitive entry, and by capturing user social data from various sources through the conduct set forth in this Complaint, including by entering into a series of anticompetitive whitelist agreements with targeted developers after scuttling its Platform; [REDACTED]

[REDACTED], Facebook was able to charge supracompetitive prices without any meaningful check.

Fourth, Facebook's conduct strengthened the DTBE, creating a protective moat around Facebook's monopoly. Facebook's conduct fortified and expanded Facebook's access [REDACTED]

FILED UNDER SEAL

832. Each of Facebook's exclusionary acts lack any procompetitive benefit / justification, let alone any justification that could outweigh the anticompetitive effects of the acts. [REDACTED]

833. The anticompetitive effects of [REDACTED], including the strengthening of Facebook's DTBE, far outweigh any procompetitive effects [REDACTED] (and the facts as alleged in this complaint demonstrate that there are none). There are likewise no procompetitive effects that outweigh the anticompetitive effects of Facebook's extended API agreements and other Platform conduct, [REDACTED] conduct. There is also no legitimate, non-pretextual technical justification for Facebook's backend integration.

834. The net effect of Facebook's anticompetitive conduct was to inflate advertising prices, including the prices paid by Plaintiffs and the Classes. In the alternative, Facebook's conduct described in this complaint had the purpose and effect of achieving a dangerous probability of a monopoly in the United States Social Advertising Market.

835. All of this has resulted in sustained and increasing supracompetitive prices for Facebook advertisements. Each of the Plaintiffs (and the persons, entities, and companies in the proposed Classes) bought Facebook advertisements at supracompetitive prices inflated by Facebook's anticompetitive scheme.

836. Plaintiffs therefore were, and are, harmed in their business and property: they were overcharged for advertising as a result of unlawful, anticompetitive conduct by Facebook.

CLASS ACTION ALLEGATIONS

837. The Classes' claims all derive directly from a course of conduct by Facebook. Facebook has engaged in uniform and standardized conduct toward the class. Facebook did not materially differentiate in its actions or inactions toward members of the class. The objective facts on these subjects

FILED UNDER SEAL

are the same for all class members. Within each Claim for Relief asserted by the class, the same legal standards govern. Accordingly, Plaintiffs bring this lawsuit as a class action on their own behalf and on behalf of all other persons similarly situated as members of the proposed class pursuant to Federal Rules of Civil Procedure 23(a) and (b)(3) and/or (b)(2) and/or (c)(4). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions.

The Pre-2018 Nationwide Advertiser Class

838. Between October 1, 2012, and April 3, 2018, Facebook advertisers, including Plaintiffs Affilious, Jessyca Frederick, Joshua Jeon, and 406 Property Services were governed by materially common terms of service, which applied generally to both commercial and non-commercial Facebook accounts during this period.

839. Plaintiffs Affilious, Jessyca Frederick, Joshua Jeon, and 406 Property Services bring this action and seek to certify and maintain it as a class action under Rules 23(a); (b)(2); and/or (b)(3); and/or (c)(4) of the Federal Rules of Civil Procedure on behalf of themselves and a Pre-2018 Nationwide Advertiser Class defined as follows:

All persons, entities, and/or corporations in the United States who purchased advertising from Facebook between December 1, 2016, and April 3, 2018, but not after April 3, 2018, and were thereby injured by anticompetitive price inflation in the Social Advertising Market (the “Pre-2018 Class Period”).

840. Excluded from the Pre-2018 Nationwide Advertiser Class is the Post-2018 Nationwide Advertiser Class, Facebook, its employees, officers, directors, legal representatives, heirs, successors, and wholly or partly owned subsidiaries or affiliates; and the judicial officers and their immediate family members and associated court staff assigned to this case.

The Post-2018 Nationwide Advertiser Class

841. Between April 4, 2018, and the present, Facebook advertisers, including Plaintiffs Mark Berney, Mark Young, and Katherine Looper, have been governed by materially common terms of service, which applied specifically to “commercial” Facebook accounts during this period.

FILED UNDER SEAL

842. Plaintiffs Mark Berney, Mark Young, and Katherine Looper, bring this action and seek to certify and maintain it as a class action under Rules 23(a); (b)(2); and/or (b)(3); and/or (c)(4) of the Federal Rules of Civil Procedure on behalf of themselves and a Post-2018 Nationwide Advertiser Class defined as follows:

All persons, entities, and/or corporations in the United States who purchased advertising from Facebook between April 4, 2018, and the present, and were thereby injured by anticompetitive price inflation in the Social Advertising Market (the “Post-2018 Class Period”).

843. Excluded from the Post-2018 Nationwide Advertiser Class is the Pre-2018 Nationwide Advertiser Class, Facebook, its employees, officers, directors, legal representatives, heirs, successors, and wholly or partly owned subsidiaries or affiliates; and the judicial officers and their immediate family members and associated court staff assigned to this case.

Numerosity and Ascertainability

844. Each class in this action satisfies the requirements of Fed. R. Civ. P. 23(a)(1). Thousands of persons, entities, and/or companies nationwide purchased advertising from Facebook in each of the Pre-2018 and Post-2018 Class Periods. Individual joinder of all Class members is impracticable.

845. The Classes are ascertainable because their members can be readily identified using Facebook accounts, Facebook Ads registrations, and other records and information kept by Facebook or third parties in the usual course of business and within their control. Plaintiffs anticipate providing appropriate notice to the certified Classes, in compliance with Fed. R. Civ. P. 23(c)(1)(2)(A) and/or (B), to be approved by the Court after class certification, or pursuant to court order under Fed. R. Civ. P. 23(d).

Predominance of Common Issues

846. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) because questions of law and fact that have common answers that are the same for each Class predominate over questions affecting only individual Class members.

847. Common issues include, without limitation, the following questions of law and fact for both the Pre-2018 and Post-2018 Nationwide Advertiser Classes:

FILED UNDER SEAL

- a. Whether Defendant monopolized the Social Advertising Market.
- b. Whether Defendant, its employees or affiliates, intended to monopolize the Social Advertising Market.
- c. Whether Defendant attempted to monopolize the Social Advertising Market.
- d. Whether Defendant possessed monopoly or market power in the Social Advertising Market.
- e. Whether user data and data obtained by third parties created a Data Targeting Barrier to Entry that protected Facebook's market position and/or monopoly, reduced competition or entry in the Social Advertising Market, and/or increased prices for products in that market, including, but not limited to, advertising sold to members of the proposed Classes.
- f. Whether Defendant's agreements with whitelisted developers violated Section 2 of the Sherman Act, including whether the agreements restrained trade or strengthened the Data Targeting Barrier to Entry.
- g. Whether [REDACTED], as described and alleged in this complaint, violates Section 2 of the Sherman Act;
- h. Whether Defendant's [REDACTED] violates Section 1 of the Sherman Act;
- i. Whether Defendant's [REDACTED] violates Section 1 of the Sherman Act;
- j. Whether Defendant's agreement with Google to reinforce and bolster Facebook's dominance in the Social Advertising Market violated Sections 1 and 2 of the Sherman Act.
- k. Whether Defendant's back-end integration is anticompetitive and violates Section 2 of the Sherman Act;
- l. Whether Defendant's conduct harmed competition in the Social Advertising Market.

FILED UNDER SEAL

1 m. Whether Defendant's conduct caused price increases or the reduction of consumer or
2 developer choice in the Social Advertising Market.

3 n. Whether Defendant's unlawful conduct was a substantial contributing factor in the
4 injury to members of the Classes.

Typicality

5
6 848. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(3) because for each proposed
7 Class, the identified Plaintiffs' claims are typical of the claims of other Class members and arise from the
8 same course of conduct by Defendant. The relief that each Class's named Plaintiffs seek is typical of the
9 relief sought for the absent Class members.

Adequate Representation

10
11 849. Plaintiffs will fairly and adequately represent and protect the interests of the Classes.
12 Plaintiffs have retained counsel with substantial experience in prosecuting antitrust and consumer class
13 actions.

14 850. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf
15 of the Classes and have the financial resources to do so. Neither Plaintiffs nor their counsel have interests
16 adverse to those of the Classes.

Superiority

17
18 851. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(2) because Defendant has
19 acted and refused to act on grounds generally applicable to the Classes, thereby making appropriate final
20 injunctive and/or corresponding declaratory relief with respect to the Classes as a whole.

21 852. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(3) because a class action is
22 superior to other available methods for the fair and efficient adjudication of this controversy. For each
23 proposed Class, the common questions of law and fact regarding Defendant's conduct and responsibility
24 predominate over any question affecting only individual Class members.

25 853. Because the damages suffered by each individual Class member may be relatively smaller
26 than the costs of litigation, the expense and burden of individual litigation would make it very difficult
27 or impossible for individual Class members to redress the wrongs done to each of them individually, such
28

FILED UNDER SEAL

1 that most or all Class members would have no rational economic interest in individually controlling the
2 prosecution of specific actions, and the burden imposed on the judicial system by individual litigation by
3 even a small fraction of the Class would be enormous, making class adjudication the superior alternative
4 under Fed. R. Civ. P. 23(b)(3)(A) for each of the proposed Classes.

5 854. For each of the proposed Classes, the conduct of this action as a class action presents far
6 fewer management difficulties, far better conserves judicial resources and the parties' resources, and far
7 more effectively protects the rights of each Class member than would piecemeal litigation. Compared to
8 the expense, burdens, inconsistencies, economic infeasibility, and inefficiencies of individualized
9 litigation, the challenges of managing this action as a class action are substantially outweighed by the
10 benefits to the legitimate interests of the parties, the court, and the public of class treatment in this Court,
11 making class adjudication superior to other alternatives, under Fed. R. Civ. P. 23(b)(3)(D).

12 855. Plaintiffs are not aware of any obstacles likely to be encountered in the management of
13 this action that would preclude its maintenance as a class action. Rule 23 provides the Court with authority
14 and flexibility to maximize the efficiencies and benefits of the class mechanism and reduce management
15 challenges. The Court may, on motion of Plaintiffs or on its own determination, certify nationwide,
16 statewide, and/or multistate classes for claims sharing common legal questions; utilize the provisions of
17 Rule 23(c)(4) to certify any particular claims, issues, or common questions of fact or law for class-wide
18 adjudication; certify and adjudicate bellwether class claims; and utilize Rule 23(c)(5) to divide any class
19 into subclasses.

REALLEGATION AND INCORPORATION BY REFERENCE

20
21 856. Plaintiffs reallege and incorporate by reference all the preceding paragraphs and
22 allegations of this Complaint, as though fully set forth in each of the following Claims for Relief asserted
23 on behalf of the Classes.

FILED UNDER SEAL**CLAIMS FOR RELIEF****COUNT I****Section 2 Sherman Act:
Monopolization**

857. Defendant has willfully acquired and maintained monopoly power in the relevant market for Social Advertising.

858. Facebook possesses monopoly power in the relevant market for Social Advertising. Facebook has the power to control prices or exclude competition in the relevant market.

859. Facebook's revenue share of the Social Advertising Market is approximately 80%; its share has been above 70% since 2015.

860. Defendant has willfully acquired and maintained monopoly power for Facebook in the relevant market for Social Advertising. As alleged in this Complaint, Defendant has accomplished this by means of predatory, exclusionary, and anticompetitive conduct, including but not limited to:

- the targeting of competitors for coercive Whitelist and Data Sharing Agreements on pain of denial of access to Facebook's Platform and APIs, including Facebook's Events APIs;

[REDACTED]

- entering into an anticompetitive agreement with Google to bolster and reinforce Facebook's dominant position in the Social Advertising Market; and

FILED UNDER SEAL

861. Defendant's conduct alleged here has had an anticompetitive effect in the relevant market for Social Advertising.

862. Defendant's conduct alleged here has no legitimate business purpose or procompetitive effect.

863. Defendant's conduct alleged here has had a substantial effect on interstate commerce.

864. Plaintiffs and the Classes have been and will be injured in their business or property as a result of Defendant's conduct alleged in this Complaint.

865. Plaintiffs and the Classes have suffered and will suffer injury of the type that the antitrust laws were intended to prevent by reason of Defendant's conduct. Plaintiffs and the Classes have been and will be injured by the harm to competition as a result of Defendant's conduct.

COUNT II**Section 2 Sherman Act:
Attempted Monopolization**

866. As alleged in this Complaint, Defendant has engaged in predatory, exclusionary, and anticompetitive conduct, including but not limited to:

- the targeting of competitors for coercive Whitelist and Data Sharing Agreements on pain of denial of access to Facebook's Platform and APIs, including Facebook's Events APIs;

FILED UNDER SEAL

- entering into an anticompetitive agreement with Google to bolster and reinforce Facebook's dominant position in the Social Advertising Market; and

-

867. Defendant's conduct alleged here has had an anticompetitive effect in the relevant market for Social Advertising.

868. Defendant's conduct alleged here has no legitimate business purpose or procompetitive effect.

869. Defendant has engaged in this conduct with the specific intent of monopolizing the relevant market for Social Advertising.

870. Defendant has engaged in this conduct with a dangerous probability of monopolizing the relevant market for Social Advertising.

871. Defendant's conduct alleged here has had a substantial effect on interstate commerce.

872. Plaintiffs and the Classes have been and will be injured in their business or property as a result of Defendant's conduct alleged in this Complaint.

873. Plaintiffs and the Classes have suffered and will suffer injury of the type that the antitrust laws were intended to prevent by reason of Defendant's conduct. Plaintiffs and the Classes have been and will be injured by the harm to competition as a result of Defendant's conduct.

COUNT III
Section 1 Sherman Act:
Restraint of Trade

FILED UNDER SEAL

874. As alleged in this Complaint, Facebook knowingly and intentionally entered into an agreement to restrict trade in order to preserve the DTBE and protect Facebook's control of social advertising. This agreement, by bolstering and reinforcing Facebook's market power and dominance in the Social Advertising Market, had the purpose and effect of maintaining market divisions and/or segmentation, allowing Facebook to continue charging a significant price premium for its targeted advertising sold in the Social Advertising Market. Because of this agreement, no fungible level of targeted advertising would emerge that could rival Facebook's ad products.

875. Defendant's conduct alleged above is a *per se* violation of Section 1 of the Sherman Act, 15 U.S.C. § 1. Plaintiffs therefore do not need to allege a relevant market. To the extent a market must be alleged, Facebook's restraint of trade has had an anticompetitive effect in the relevant market of Social Advertising in the United States.

876. Defendant's conduct alleged here has no legitimate business purpose or procompetitive effect.

877. Defendant's conduct has had a substantial effect on interstate commerce.

878. Plaintiffs and the Classes have been and will be injured in their business or property as a result of Defendant's conduct alleged here.

879. Plaintiffs and the Classes have suffered and will suffer injury of the type that the antitrust laws were intended to prevent by reason of Defendant's conduct. Plaintiffs and the Classes have been and will be injured by the harm to competition as a result of Defendant's conduct.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request that judgment be entered against Defendant and that the Court grant the following:

A. Determine that this action may be maintained as a class action pursuant to Rules 23(a), (b)(2), (b)(3) and/or (c)(4) of the Federal Rules of Civil Procedure, and direct that reasonable notice of this action, as provided by Rule 23(c)(2), be given to the Classes, and declare Plaintiffs as the representatives of the Classes;

B. Enter a judgment against Defendant in favor of Plaintiffs and the Classes;

FILED UNDER SEAL

- 1 C. Award the Classes damages (i.e., three times their damages) in amount to be determined
2 at trial;
- 3 D. Award actual, compensatory, statutory, and consequential damages;
- 4 E. Award equitable monetary relief, including restitution and disgorgement of all ill-gotten
5 gains, and the imposition of a constructive trust upon, or otherwise restricting the
6 proceeds of Defendant's ill-gotten gains, to ensure an effective remedy;
- 7 F. Award pre-judgment and post-judgment interest at the highest rate allowed by law;
- 8 G. Award Plaintiffs and the Classes their costs of suit, including reasonable attorneys' fees
9 as provided by law; and
- 10 H. Award such further and additional relief as the case may require and the Court may deem
11 just and proper under the circumstances.

JURY DEMAND

12
13 Plaintiffs demand a trial by jury on all claims so triable as a matter of right.
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FILED UNDER SEAL

1 Dated: February 28, 2022

2 Respectfully submitted,

SCOTT + SCOTT ATTORNEYS AT LAW LLP**BATHAE DUNNE LLP**

3 /s/ Kristen M. Anderson

4 /s/ Yavar Bathaee

5 Kristen M. Anderson (CA 246108)

6 Yavar Bathaee (CA 282388)

7 kanderson@scott-scott.com

8 yavar@bathaeedunne.com

9 The Helmsley Building

Edward M. Grauman (*pro hac vice*)

10 230 Park Avenue, 17th Floor

egrauman@bathaeedunne.com

11 New York, NY 10169

Andrew C. Wolinsky

12 Tel.: (212) 223-6444

awolinsky@bathaeedunne.com

13 Fax: (212) 223-6334

445 Park Avenue, 9th Floor

New York, NY 10022

Tel.: (332) 322-8835

14 Christopher M. Burke (CA 214799)

15 cburke@scott-scott.com

16 David H. Goldberger (CA 225869)

Brian J. Dunne (CA 275689)

17 dgoldberger@scott-scott.com

bdunne@bathaeedunne.com

18 Kate Lv (CA 302704)

633 West Fifth Street, 26th Floor

19 klv@scott-scott.com

Los Angeles, CA 90071

20 Hal D. Cunningham (CA 243048)

Tel.: (213) 462-2772

21 hcunningham@scott-scott.com

22 Daniel J. Brockwell (CA 335983)

LEVIN SEDRAN & BERMAN LLP

23 dbrockwell@scott-scott.com

Keith J. Verrier (*pro hac vice*)

24 600 W. Broadway, Suite 3300

Austin B. Cohen (*pro hac vice*)

25 San Diego, CA 92101

510 Walnut Street, Suite 500

26 Tel.: (619) 233-4565

Philadelphia, PA 19106-3997

27 Fax: (619) 233-0508

Tel.: (215) 592-1500

Fax: (215) 592-4663

kverrier@lfsblaw.com

acohen@lfsblaw.com

28 Patrick J. McGahan (*pro hac vice*)

pmcgahan@scott-scott.com

Michael P. Srodoski (*pro hac vice*)

AHDOOT & WOLFSON, PC

msrodoski@scott-scott.com

Tina Wolfson (CA 174806)

156 South Main Street, P.O. Box 192

Robert Ahdoot (CA 172098)

Colchester, CT 06415

Theodore W. Maya (CA 223242)

Tel.: (860) 537-5537

Henry J. Kelson (*pro hac vice*)

Fax: (860) 537-4432

2600 West Olive Avenue, Suite 500

Burbank, CA 91505

Telephone: (310) 474-9111

Facsimile: (310) 474-8585

twolfson@ahdootwolfson.com

rahdoot@ahdootwolfson.com

tmaya@ahdootwolfson.com

*Interim Co-Lead Counsel and Executive Committee
for the Advertiser Class*

FILED UNDER SEAL

ATTESTATION OF YAVAR BATHAE

This document is being filed through the Electronic Case Filing (ECF) system by Yavar Bathae, who attests that he has obtained concurrence in the filing of this document from each of the attorneys identified on the caption page and in the signature block.

Dated: February 28, 2022

/s/ Yavar Bathae
Yavar Bathae

ATTACHMENT C

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

HAGENS BERMAN SOBOL SHAPIRO LLP

Shana E. Scarlett (SBN 217895)
715 Hearst Avenue, Suite 202
Berkeley, CA 94710
Telephone: (510) 725-3000
Facsimile: (510) 725-3001
shanas@hbsslaw.com

BATHAE DUNNE LLP

Yavar Bathaee (Bar No. 282388)
yavar@bathaeedunne.com
445 Park Avenue, 9th Floor
New York, NY 10022
Telephone: (332) 322-8835

**QUINN EMANUEL URQUHART & SULLIVAN,
LLP**

Stephen A. Swedlow (admitted *pro hac vice*)
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
stephenswedlow@quinnemanuel.com

SCOTT + SCOTT ATTORNEYS AT LAW LLP

Kristen M. Anderson (Bar No. 246108)
kanderson@scott-scott.com
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: (212) 223-6444

Interim Co-Lead Advertiser Class Counsel

Interim Co-Lead Consumer Class Counsel

[Additional Counsel Listed in Signature Block]

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION**

MAXIMILLIAN KLEIN, *et al.*,

Plaintiffs,

v.

META PLATFORMS, INC.,

Defendant.

Case No. 3:20-cv-08570-JD

STIPULATED PROTECTIVE ORDER

Judge: Hon. James Donato

1 **1. PURPOSES AND LIMITATIONS**

2 Disclosure and discovery activity in this action are likely to involve production of confidential,
3 proprietary, or private information for which special protection from public disclosure and from use
4 for any purpose other than prosecuting this litigation may be warranted. Accordingly, the parties
5 hereby stipulate to and petition the court to enter the following Stipulated Protective Order. The parties
6 acknowledge that this Order does not confer blanket protections on all disclosures or responses to
7 discovery and that the protection it affords from public disclosure and use extends only to the limited
8 information or items that are entitled to confidential treatment under the applicable legal principles.
9 The parties further acknowledge, as set forth in Section 11.4, below, that this Stipulated Protective
10 Order does not entitle them to file confidential information under seal; Civil Local Rule 79-5 sets forth
11 the procedures that must be followed and the standards that will be applied when a party seeks
12 permission from the court to file material under seal.

13 **2. DEFINITIONS**

14 2.1 Objecting Party: a Party that challenges the designation of information or items under
15 this Order.

16 2.2 Competitive Decision-Making: decision-making relating to a competitor, potential
17 competitor, customer, or distribution partner including decisions regarding contracts, marketing,
18 pricing, product or service development or design, product or service offerings, research and
19 development, mergers and acquisitions, or licensing, acquisition, or enforcement of intellectual
20 property rights.

21 2.3 "CONFIDENTIAL" Information or Items: any trade secret or other confidential
22 research, development, or commercial information, as such terms are used in Fed. R. Civ. P.
23 26(c)(1)(G), or any document, transcript, or other material containing such information that has not
24 been published or otherwise made publicly available in violation of this Order. In addition, a
25 Designating Party may designate as Confidential any information or items made publicly available in
26 violation of a court order to keep such information confidential, that the Designating Party believes
27 should receive Confidential treatment, in accordance with Section 3.2 below. Confidential information
28 includes (i) information copied or extracted, summarized or compiled from Confidential Information,

and (ii) testimony, conversations, or presentations by Parties or their Counsel that might reveal Confidential Information.

2.4 Counsel (without qualifier): Outside Counsel and In-House Counsel (as well as their support staff).

2.5 Designated In-House Counsel: means In-House Counsel designated by Defendant who are authorized to access Confidential Information pursuant to Section 7.2(b) or Highly Confidential Information pursuant to Section 7.3(b).

2.6 Designating Party: a Party or Non-Party that designates information or items that it produces in disclosures or in responses to discovery as “CONFIDENTIAL” or “HIGHLY CONFIDENTIAL.”

2.7 Disclosure or Discovery Material: all items or information, regardless of the medium or manner in which it is generated, stored, or maintained (including, among other things, testimony, transcripts, and tangible things), that are produced or generated in disclosures or responses to discovery in this matter.

2.8 Expert: a person with specialized knowledge or experience in a matter pertinent to the litigation, including employees of the firm with which the expert is associated or independent contractors who assist the expert’s work in this action, who has been retained by a Party or its Counsel to serve as an expert witness or as a consultant in this action.

2.9 “HIGHLY CONFIDENTIAL” Information or Items: “Confidential Information or Items,” disclosure of which to another Party or Non-Party is likely to cause material and significant harm. This includes (i) information copied or extracted, summarized or compiled from Highly Confidential Information, and (ii) testimony, conversations, or presentations by Protected Persons or their Counsel that might reveal Highly Confidential Information.

2.10 In-House Counsel: any attorneys who are employees of a party to this action, as well as paralegals, secretaries, and clerical and administrative personnel employed by a party. In-House Counsel excludes Outside Counsel.

2.11 Non-Party: any natural person, partnership, corporation, association, or other legal entity not named as a Party to this action.

2.12 Outside Counsel: attorneys employed by outside law firms representing a Party in this proceeding, as well as attorney support staff.

2.13 Party: any named party to this action, including all of its officers, directors, employees, consultants, retained experts, and Outside Counsel (and their support staffs).

2.14 Producing Party: a Party or Non-Party that produces Disclosure or Discovery Material in this action.

2.15 Professional Vendors: persons or entities that provide litigation support services (e.g., photocopying, videotaping, translating, preparing exhibits or demonstrations, and organizing, storing, or retrieving data in any form or medium) and their employees and subcontractors.

2.16 Protected Material: any Disclosure or Discovery Material that is designated as “CONFIDENTIAL,” or as “HIGHLY CONFIDENTIAL.”

2.17 Protected Person: any Person (including a Party or Non-Party) that either voluntarily or under compulsory process, has provided or provides Protected Material.

2.18 Receiving Party: a Party that receives Disclosure or Discovery Material from a Producing Party.

3. SCOPE

3.1 The protections conferred by this Stipulation and Order cover not only Protected Material (as defined above), but also (1) any information copied or extracted from Protected Material; (2) all copies, excerpts, summaries, or compilations of Protected Material; and (3) any testimony, conversations, or presentations by Parties or their Counsel that might reveal Protected Material. However, the protections conferred by this Stipulation and Order do not cover the following information: (a) any information that is in the public domain at the time of disclosure to a Receiving Party or becomes part of the public domain after its disclosure to a Receiving Party either (1) as a result of publication not in violation of this Order, including becoming part of the public record through trial or otherwise or (2) as a result of publication not in violation of another court’s order to keep such information confidential, subject to Section 3.2 below; and (b) any information known to the Receiving Party prior to the disclosure or obtained by the Receiving Party after the disclosure from a source who obtained the information lawfully and under no obligation of confidentiality to the Designating Party.

1 Disclosure at trial or at any evidentiary hearing of any document, testimony, or other material
2 designated as Highly Confidential Information or Confidential Information will be governed pursuant
3 to a separate court order. In advance of the filing of a proposed order governing the disclosure of
4 Highly Confidential Information or Confidential Information at trial or any evidentiary hearing, the
5 Parties shall provide notice of such order to Non-Parties whose Highly Confidential Information or
6 Confidential Information is expected to be used at trial or any evidentiary hearing.

7 3.2 Any party or Non-Party may designate as confidential any information or items that it
8 believes should receive confidential treatment. If a Producing Party's confidential material has been
9 published by someone other than the Producing Party in violation of another court's order, and the
10 Producing Party is aware of such publication, it should promptly notify the Receiving Party that it
11 continues to request confidential treatment of the material in this action. If the Receiving Party
12 disagrees that the material should continue to be treated as confidential, it may challenge the
13 designation pursuant to Sections 6.1-6.3 of this Order. If a Party receives material from a Non-Party
14 that bears obvious indicia that it is the confidential information of a Party, the Party who receives such
15 material should make appropriate inquiries, including of the Party whose information it appears to be,
16 regarding whether the material is confidential before choosing to treat it as public. Any disputes about
17 whether such material should continue to be treated as confidential may be resolved using the
18 procedures in Sections 6.1-6.3 of this Order.

19 **4. DURATION**

20 Even after final disposition of this litigation, the confidentiality obligations imposed by this
21 Order shall remain in effect until a Designating Party agrees otherwise in writing or a court order
22 otherwise directs. Final disposition shall be deemed to be the later of (1) dismissal of all claims and
23 defenses in this action, with or without prejudice; and (2) final judgment herein after the completion
24 and exhaustion of all appeals, rehearings, remands, trials, or reviews of this action, including the time
25 limits for filing any motions or applications for extension of time pursuant to applicable law.

5. DESIGNATING PROTECTED MATERIAL

5.1 Exercise of Restraint and Care in Designating Material for Protection. Each Party or Non-Party that designates information or items for protection under this Order must take care to limit any such designation to specific material that qualifies under the appropriate standards.

Mass, indiscriminate, or routinized designations by any Party are prohibited. Designations by any Party that are shown to be clearly unjustified or that have been made for an improper purpose (e.g., to unnecessarily encumber or retard the case development process or to impose unnecessary expenses and burdens on other parties) expose the Designating Party to sanctions.

If it comes to a Designating Party's attention that information or items that it designated for protection do not qualify for protection, that Designating Party must promptly notify all other Parties that it is withdrawing the mistaken designation.

5.2 Manner and Timing of Designations. Except as otherwise provided in this Order (see, e.g., second paragraph of Section 5.2(a) below), or as otherwise stipulated or ordered, Disclosure or Discovery Material that qualifies for protection under this Order must be clearly so designated before the material is disclosed or produced.

Designation in conformity with this Order requires:

- (a) for information in documentary form (e.g., paper or electronic documents, but excluding transcripts of depositions or other pretrial or trial proceedings), that the Producing Party affix the legend "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL" to every page of the document. Any document that contains Protected Material may be designated as CONFIDENTIAL or HIGHLY CONFIDENTIAL in its entirety, in accordance with this Order.

Defendant, as a Party, is not required to re-review its productions to the Federal Trade Commission and the House Judiciary Committee to designate materials, and may re-produce such productions to Plaintiffs as Highly Confidential. However, to the extent that Facebook produces any documents in such productions in *State of New York et al v. Facebook, Inc.*, Case No. 1:20-cv-03589-JEB (D.D.C.) ("State AG Case") or *Federal Trade Commission v. Facebook, Inc.*, Case No. 1:20-cv-03590-JEB (D.D.C.) ("FTC Case"), with a lower confidentiality designation (*i.e.*, "Confidential" or

not designated), Facebook shall timely re-produce such documents in this case, to reflect the lower confidentiality designation or non-designation in the State AG or FTC Cases. In addition, Plaintiffs may challenge the designation of any documents Facebook produced to the Federal Trade Commission and the House Judiciary Committee, and re-produced here as Confidential or Highly Confidential, pursuant to Section 6 herein, but agree not to challenge the designation of such documents wholesale, on the basis that their designation was mass, indiscriminate, or routinized.

(b) for testimony given in deposition or in other pretrial or trial proceedings, a Protected Person shall have 30 days after the date when a complete and final copy of the transcript has been made available to identify the specific portions of the testimony as to which protection is sought and to specify the level of protection being asserted. Within five (5) business days of receipt of the final transcript, the Party who notices the deposition shall provide the final transcript to the deponent. Only those portions of the testimony that are appropriately designated for protection within the 30 days shall be covered by the provisions of this Stipulated Protective Order. Alternatively, when it is impractical to identify separately each portion of testimony that is entitled to protection and it appears that substantial portions of the testimony may qualify for protection, a Designating Party may specify that the entire transcript shall be treated as “CONFIDENTIAL” or “HIGHLY CONFIDENTIAL.” When a Party is entitled to question a deponent about a document or information that has been designated as “CONFIDENTIAL” or “HIGHLY CONFIDENTIAL,” the Party that asked such question shall also mark as either “CONFIDENTIAL” or “HIGHLY CONFIDENTIAL” the portion of the transcript relating to such CONFIDENTIAL or HIGHLY CONFIDENTIAL document or information.

Parties shall give the other parties notice if they reasonably expect a deposition, hearing or other proceeding to include Protected Material so that the other parties can ensure that only authorized individuals who have signed the “Acknowledgment and Agreement to Be Bound” (Exhibit A) are present at the time Protected Material is discussed. The use of a document as an exhibit at a deposition shall not in any way affect its designation as “CONFIDENTIAL” or “HIGHLY CONFIDENTIAL.”

Transcripts containing Protected Material shall have an obvious legend on the title page that the transcript contains Protected Material, and the title page shall be followed by a list of all pages (including line numbers as appropriate) that have been designated as Protected Material and the level of protection being asserted by the Designating Party. The Designating Party shall inform the court reporter of these requirements. Any transcript that is prepared before the expiration of a 30-day period for designation shall be treated during that period as if it had been designated “HIGHLY CONFIDENTIAL”. After the expiration of that period, the transcript shall be treated only as actually designated.

- (c) for information produced in some form other than documentary and for any other tangible items, that the Producing Party affix in a prominent place on the exterior of the container or containers in which the information or item is stored the legend “CONFIDENTIAL” or “HIGHLY CONFIDENTIAL.”

5.3 Inadvertent Failures to Designate. If timely corrected, an inadvertent failure to designate qualified information or items does not, standing alone, waive the Designating Party’s right to secure protection under this Order for such material. Upon timely correction of a designation, the Receiving Party must make reasonable efforts to assure that the material is treated in accordance with the provisions of this Order.

6. CHALLENGING CONFIDENTIALITY DESIGNATIONS

6.1 Timing of Challenges. Any Party may challenge a designation of confidentiality at any time prior to 30 days before the first day of trial. Unless a prompt challenge to a Designating Party’s confidentiality designation is necessary to avoid foreseeable, substantial unfairness, unnecessary economic burdens, or a significant disruption or delay of the litigation, a Party does not waive its right to challenge a confidentiality designation by electing not to mount a challenge promptly after the original designation is disclosed.

6.2 Meet and Confer. The Objecting Party shall initiate the dispute resolution process by providing written notice of each designation it is challenging and stating with particularity the basis for each challenge. To avoid ambiguity as to whether a challenge has been made, the written notice must recite that the challenge to confidentiality is being made in accordance with this specific

paragraph of the Protective Order. The Objecting Party and Designating Party shall attempt to resolve each challenge in good faith and must begin the process by conferring directly (in voice to voice dialogue; other forms of communication are not sufficient) within 14 days of the date of service of notice. In conferring, the Objecting Party must explain the basis for its belief that the confidentiality designation was not proper and must give the Designating Party an opportunity to review the designated material, to reconsider the circumstances, and, if no change in designation is offered, to explain the basis for the chosen designation. The Objecting Party may proceed to the next stage of the challenge process only if it has engaged in this meet and confer process first or establishes that the Designating Party is unwilling to participate in the meet and confer process in a timely manner.

6.3 Judicial Intervention. If the Parties cannot resolve a challenge without court intervention, they shall comply with the discovery dispute resolution procedure outlined in Judge Donato's Standing Order for Civil Discovery. Failure by the parties to seek court intervention within the period set out in the Standing Order for Civil Cases shall not automatically waive the confidentiality designation for each challenged designation. In addition, the Objecting Party may seek relief with respect to a confidentiality designation at any time if there is good cause for doing so, including a challenge to the designation of a deposition transcript or any portions thereof. In any such discovery letter brought pursuant to this provision the parties shall attest that they have complied with the meet and confer requirements imposed in the preceding paragraph.

The burden of persuasion in any such challenge proceeding shall be on the Designating Party. Frivolous challenges and those made for an improper purpose (e.g., to harass or impose unnecessary expenses and burdens on other parties) may expose the Objecting Party to sanctions. All parties shall continue to afford the material in question the level of protection to which it is entitled under the Producing Party's designation until the court rules on the challenge.

If the Court finds the designation of Highly Confidential Information or Confidential Information to have been inappropriate, the challenged designation shall be considered rescinded, however, in the case of Highly Confidential Information the Court (or Objecting Party and Designating Party, by agreement, absent a contrary ruling from the Court) may determine that the materials may appropriately be designated Confidential.

7. ACCESS TO AND USE OF PROTECTED MATERIAL

7.1 Basic Principles. A Receiving Party may use Protected Material that is disclosed or produced by another Party or by a Non-Party in connection with this case only for prosecuting, defending, or attempting to settle this litigation. Such Protected Material may be disclosed only to the categories of persons and under the conditions described in this Order. When the litigation has been terminated, a Receiving Party must comply with the provisions of Section 12 below (FINAL DISPOSITION).

Protected Material must be stored and maintained by a Receiving Party at a location and in a secure manner that ensures that access is limited to the persons authorized under this Order.

7.2 Disclosure of “CONFIDENTIAL” Information or Items. Unless otherwise ordered by the court or permitted in writing by the Designating Party, a Receiving Party may disclose any information or item designated “CONFIDENTIAL” only to:

- (a) the Receiving Party’s Outside Counsel, as well as attorney support staff who have signed the “Acknowledgment and Agreement to Be Bound” that is attached hereto as Exhibit A;
- (b) four Designated In-House Counsel of the Receiving Party with responsibilities for the litigation of this Action who do not currently, and for a period of two (2) years following the last occasion on which Confidential Information is disclosed to such In-House Counsel shall not (a) participate in or advise on Defendant's Competitive Decision-Making whether such In-House Counsel are still employed by Defendant or are employed by a different employer (b) participate in or advise on Competitive Decision-Making involving a Protected Person whose Confidential Information they accessed during the course of this Action at any employer, or (c) participate or advise on litigation or other legal actions (aside from litigation arising from or related to the allegations in the Complaint in this action) on behalf of Defendant or any other employer where a Protected Person is a genuinely adverse party (i.e., a party whose interests are more than merely nominally adverse, typified by responding to a Protected Party’s subpoena) and whose Confidential Information Designated In-House Counsel accessed in the

1 course of this Action; to qualify for access under this subpart, in-house litigation
2 counsel shall first execute an In-House Counsel Agreement Concerning Confidentiality
3 in the form of Exhibit B attached hereto (which executed versions shall be maintained
4 by Outside Counsel for the relevant Defendant and available for inspection upon the
5 request of the Court, any Party, or any Non-Party Protected Person) and only access
6 Confidential Information in person at the offices of Defendant's Outside Counsel of
7 Record, or using a secure electronic data room or document review platform using an
8 individual login identification and password. Defendant shall promptly report any
9 confirmed or suspected unauthorized use or disclosure of Confidential Information to
10 the Court, Plaintiff, and any affected Non-Party Protected Person. Any Counsel subject
11 to this subsection who leaves the employment of Defendant to work in an industry
12 unrelated to the decisions associated with Competitive Decision-Making shall be
13 presumed to be exempt from the post-employment limits of this provision absent a
14 showing by Plaintiff or any interested Protected Person that such a person engaged in
15 Competitive Decision-Making.

- 16 (c) an individual named plaintiff or class representative to whom disclosure is reasonably
17 necessary for this litigation and who has signed the "Acknowledgment and Agreement
18 to Be Bound" (Exhibit A), provided that such person shall not take possession of such
19 information, and provided that such person has no involvement in decision-making for
20 a competitor of Facebook;
- 21 (d) Experts (as defined in this Order) of the Receiving Party to whom disclosure is
22 reasonably necessary for this litigation and who have signed the "Acknowledgment and
23 Agreement to Be Bound" (Exhibit A);
- 24 (e) the court and its personnel;
- 25 (f) court reporters and their staff, professional jury or trial consultants, and Professional
26 Vendors to whom disclosure is reasonably necessary for this litigation and who have
27 signed the "Acknowledgment and Agreement to Be Bound" (Exhibit A);
- 28

- 1 (g) during depositions, a Party or Non-Party witness in the action, who the Confidential
2 Information or Items indicate, or who the Receiving Party has a good-faith basis to
3 believe, was the author, addressee, recipient, custodian, or source of the document, to
4 the extent he or she previously had lawful access to the document disclosed or to be
5 disclosed; any witness for whom the Receiving Party believes in good faith previously
6 received or had access to the document, unless counsel for the Designating Party or the
7 witness indicates that he or she did not have access to the document; and any witness
8 to whom disclosure is reasonably necessary and who has signed the “Acknowledgment
9 and Agreement to Be Bound” (Exhibit A). These restrictions shall apply unless
10 otherwise agreed by the Designating Party or ordered by the court; and
- 11 (h) any mediator or arbitrator that the Parties engage in this action or that the court appoints
12 who has signed the “Acknowledgment and Agreement to Be Bound” (Exhibit A).

13 7.3 Disclosure of “HIGHLY CONFIDENTIAL” information or Items. Unless otherwise
14 ordered by the court or permitted in writing by the Designating Party, a Receiving Party may disclose
15 any information or item designated “HIGHLY CONFIDENTIAL” only to:

- 16 (a) the Receiving Party’s Outside Counsel, as well as attorney support staff to whom it is
17 reasonably necessary to disclose the information for this litigation and who have signed
18 the “Acknowledgment and Agreement to Be Bound” that is attached hereto as
19 Exhibit A;
- 20 (b) two Designated In-House Counsel of Defendant with responsibilities for the litigation
21 of this Action who do not, at the time of executing the Designated In-House Counsel
22 Agreement Concerning Confidentiality in the form of Exhibit B attached hereto, and
23 for a period of two (2) years following the last occasion on which Highly Confidential
24 Information is disclosed to such In-House Counsel, shall not (a) participate in or advise
25 on Defendant's Competitive Decision-Making, whether such In-House Counsel are still
26 employed by Defendant or are employed by a different employer, (b) participate in or
27 advise on Competitive Decision-Making involving a Protected Person whose Highly
28 Confidential Information they accessed during the course of this Action at any

1 employer, or (c) participate in or advise on litigation or other legal actions (aside from
2 litigation arising from or related to the allegations in the Complaint in this action) on
3 behalf of Defendant or any other employer where a Protected Person is a genuinely
4 adverse party (i.e., a party whose interests are more than merely nominally adverse,
5 typified by responding to a Protected Party's subpoena) and whose Highly Confidential
6 Information Designated In-House Counsel accessed in the course of this Action; to
7 qualify for access under this subpart, in-house litigation counsel shall first execute a
8 Designated In-House Counsel Agreement Concerning Confidentiality in the form of
9 Exhibit B attached hereto (which executed version shall be maintained by Outside
10 Counsel for the relevant Defendant and available for inspection upon the request of the
11 Court, any Party, or any Non-Party Protected Person) and only access Highly
12 Confidential Information in person at the offices of Defendant's Outside Counsel of
13 Record, or using a secure electronic data room or document review platform using an
14 individual login identification and password. Defendant shall promptly report any
15 confirmed or suspected unauthorized use or disclosure, of Highly Confidential
16 Information, to the Court, Plaintiff, and any affected Non-Party Protected Person. Any
17 Counsel subject to this subsection who leaves the employment of Defendant to work in
18 an industry unrelated to the decisions associated with Defendant's Competitive
19 Decision-Making shall be presumed to be exempt from the post-employment limits of
20 this provision absent a showing by Plaintiff or any interested Protected Person that such
21 a person is engaged in Competitive Decision-Making;

22 (c) Experts (as defined in this Order) of the Receiving Party to whom disclosure is
23 reasonably necessary for this litigation and who have signed the "Acknowledgment and
24 Agreement to Be Bound" (Exhibit A);

25 (d) the court and its personnel;

26 (e) court reporters and their staff, professional jury or trial consultants, and Professional
27 Vendors to whom disclosure is reasonably necessary for this litigation and who have
28 signed the "Acknowledgment and Agreement to Be Bound" (Exhibit A);

(f) during depositions, a Party or Non-Party witness in the action, who the Highly Confidential Information or Items indicate, or who the Receiving Party has a good-faith basis to believe, was the author, addressee, recipient, custodian, or source of the document, to the extent he or she previously had lawful access to the document disclosed or to be disclosed; and any witness for whom the Receiving Party believes in good faith previously received or had access to the document, unless counsel for the Designating Party or the witness indicates that he or she did not have access to the document, or unless otherwise agreed by the Designating Party or ordered by the court; and

(g) any mediator or arbitrator that the Parties engage in this action or that the court appoints who has signed the “Acknowledgment and Agreement to Be Bound” (Exhibit A).

7.4 Rendering Advice: Nothing in this Order is intended to bar or otherwise prevent counsel from rendering advice to their respective clients with respect to this action and, in the course of rendering such advice in a manner consistent with the “Designated In-House Counsel” provisions Sections 7.2(b) and 7.3(b), from relying upon their examination or knowledge of Highly Confidential or Confidential Information. Procedures for Approving or Objecting to Disclosure of “HIGHLY CONFIDENTIAL” or “CONFIDENTIAL” Information or Items to Designated In-House Counsel.

7.5 Until otherwise ordered by the court or agreed to in writing by the Protected Person, seven (7) days before disclosing any information designated as Highly Confidential Information or Confidential Information to the Defendant’s Designated In-House Counsel, Defendant must submit in writing to Plaintiff and the Protected Person a written statement that (i) sets forth the full name of the Designated In-House Counsel and the city and state of his or her residence, (ii) describes the In-House Counsel's past, current, and reasonably foreseeable future primary job duties and responsibilities in sufficient detail to determine if In-House Counsel is involved, or may become involved, in any Competitive Decision-Making; and (iii) lists the litigations or other legal actions in which the In-House Counsel participates or advises on behalf of Defendant or any other employer.

7.6 Unless otherwise ordered by the court or agreed to in writing by the Protected Person, Defendant may at any time before trial identify Designated In-House Counsel to whom Highly

1 Confidential or Confidential Information or Items may be disclosed. To qualify for access under this
2 subpart, Designated In-House Counsel shall execute a Designated In-House Counsel Agreement
3 Concerning Confidentiality in the form of Exhibit B attached hereto (which executed versions shall be
4 maintained by Outside Counsel for Defendant and available for inspection upon the request of the
5 Court, any Party, or any non-Party Protected Person).

6 7.7 A Party that makes a request and provides the information specified in the preceding
7 respective paragraphs may disclose Highly Confidential or Confidential Information to the identified
8 Designated In-House Counsel unless, within 14 days of delivering a copy of Exhibit B, the Party
9 receives a written objection from the Protected Person. Any such objection must set forth in detail the
10 grounds on which it is based.

11 7.8 A Party that receives a timely written objection must meet and confer with the Protected
12 Person (through direct voice to voice dialogue) to try to resolve the matter by agreement within seven
13 days of the written objection. If no agreement is reached, the parties shall comply with the discovery
14 dispute resolution procedure outlined in Judge Donato's Standing Order for Civil Discovery. Any
15 discovery letter filed pursuant to this provision must describe the circumstances with specificity, set
16 forth in detail the reasons why the disclosure to Designated In-House Counsel is reasonably necessary,
17 assess the risk of harm that the disclosure would entail, and suggest any additional means that could
18 be used to reduce that risk. In addition, any such letter must describe the parties' efforts to resolve the
19 matter by agreement (i.e., the extent and the content of the meet and confer discussions) and set forth
20 the reasons advanced by the Protected Person for its refusal to approve the disclosure. Defendant shall
21 not disclose any Highly Confidential or Confidential Information to its In-House Counsel pending
22 resolution of the dispute. If the Court finds that the Designated In-House Counsel qualifies under the
23 provisions of Section 7.2(b) or 7.3(b), Defendant will be able to disclose Highly Confidential
24 Information or Confidential Information, as appropriate, to its Designated In-House Counsel in
25 accordance with Section 7.2(b) or 7.3(b).

26 In any such proceeding, the Party opposing disclosure to Designated In-House Counsel shall
27 bear the burden of proving that the risk of harm that the disclosure would entail (under the safeguards
28

proposed) outweighs the Receiving Party's need to disclose the Protected Material to its Designated In-House Counsel.

7.9 Defendant may at any time before the trial of this action request disclosure of Highly Confidential or Confidential Information to additional In-House Counsel by consent of the Protected Person who made such designation (the "Designating Party") or motion to the Court. Defendant shall provide a written notice to the Designating Party and all Parties to this action stating the basis for disclosure. Defendant and the Designating Party must meet and confer within seven days of the written notice to try to resolve the matter by agreement. If no agreement is reached, the parties shall comply with the discovery dispute resolution procedures outlined in Judge Donato's Standing Order for Civil Discovery. Defendant will not disclose any Highly Confidential or Confidential Information to additional In-House Counsel pending resolution of the dispute. If the Court finds the designated In-House Counsel has a particularized need for access to the Highly Confidential or Confidential Information that outweighs the risk of harm to the Designating Party or the public interest, Defendant will be able to disclose the Highly Confidential or Confidential Information to its designated In-House Counsel.

8. PROTECTED MATERIAL SUBPOENAED OR ORDERED PRODUCED IN OTHER LITIGATION

Parties may not disclose Highly Confidential or Confidential Information in other litigation absent a valid subpoena or court order. If a Party is served with a subpoena or a court order issued in other litigation that compels disclosure of any information or items designated in this action as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL" that Party must:

8.1 promptly notify in writing the Designating Party. Such notification shall include a copy of the subpoena or court order;

8.2 promptly notify in writing the party who caused the subpoena or order to issue in the other litigation that some or all of the material covered by the subpoena or order is subject to this Protective Order. Such notification shall include a copy of this Stipulated Protective Order; and cooperate with respect to all reasonable procedures sought to be pursued by the Designating Party whose Protected Material may be affected.

1 If the Designating Party timely seeks a protective order, the Party served with the subpoena or
2 court order shall not produce any information designated in this action as “CONFIDENTIAL” or
3 “HIGHLY CONFIDENTIAL” before a determination by the court from which the subpoena or order
4 issued, unless the Party has obtained the Designating Party’s permission. The Designating Party shall
5 bear the burden and expense of seeking protection in that court of its Protected Material – and nothing
6 in these provisions should be construed as authorizing or encouraging a Receiving Party in this action
7 to disobey a lawful directive from another court.

8 **9. A NON-PARTY’S PROTECTED MATERIAL SOUGHT TO BE PRODUCED IN THIS**
9 **LITIGATION**

- 10 (a) The terms of this Order are applicable to information produced by a Non-Party in this
11 action and designated as “CONFIDENTIAL” or “HIGHLY CONFIDENTIAL.” Such
12 information produced by Non-Parties in connection with this litigation is protected by
13 the remedies and relief provided by this Order. Nothing in these provisions should be
14 construed as prohibiting a Non-Party from seeking additional protections.
- 15 (b) In the event that a Party is required, by a valid subpoena, court order, or discovery
16 request to produce a Non-Party’s confidential information in its possession, and the
17 Party is subject to an agreement with the Non-Party not to produce the Non-Party’s
18 confidential information, then the Party shall:
- 19 1. promptly notify in writing the Requesting Party and the Non-Party that some or
20 all of the information requested is subject to a confidentiality agreement with a
21 Non-Party;
 - 22 2. promptly provide the Non-Party with a copy of the Stipulated Protective Order
23 in this litigation, the relevant discovery request(s), and a reasonably specific
24 description of the information requested; and
- 25 (c) make the information requested available for inspection by the Non-Party. This
26 provision is without waiver of a Party’s right to object to any discovery request or
27 subpoena seeking a Non-Party’s confidential information in its possession.
- 28

9.2 A Non-Party must object or seek a protective order within 14 days of receiving notice and accompanying information, as described in section 9(b). If the Non-Party fails to timely object or seek a protective order from this court, the Receiving Party may produce the Non-Party's confidential information responsive to the discovery request, except that, if the Party from whom the discovery is sought has a contractual obligation to give a longer period of notice to the Non-Party, the Party shall so advise the Party requesting the discovery, and the Producing Party shall have no obligation to produce the Non-Party's material until the contractual notice period expires. If the Non-Party timely seeks a protective order, the Receiving Party shall not produce any information in its possession or control that is subject to the confidentiality agreement with the Non-Party before a determination by the court.¹ Absent a court order to the contrary, the Non-Party shall bear the burden and expense of seeking protection in this court of its Protected Material.

10. UNAUTHORIZED DISCLOSURE OF PROTECTED MATERIAL

If a Receiving Party learns that, by inadvertence or otherwise, it has disclosed Protected Material to any person or in any circumstance not authorized under this Stipulated Protective Order, the Receiving Party must immediately (a) notify in writing the Protected Person of the unauthorized disclosures, (b) use its best efforts to retrieve all unauthorized copies of the Protected Material, (c) inform the person or persons to whom unauthorized disclosures were made of all the terms of this Order, and (d) request such person or persons to execute the "Acknowledgment and Agreement to Be Bound" that is attached hereto as Exhibit A.

11. MISCELLANEOUS

11.1 Right to Further Relief. Nothing in this Order abridges the right of any person to seek its modification by the court in the future.

11.2 Right to Assert Other Objections. By stipulating to the entry of this Protective Order no Party waives any right it otherwise would have to object to disclosing or producing any information or

¹ The purpose of this provision is to alert the interested parties to the existence of confidentiality rights of a Non-Party and to afford the Non-Party an opportunity to protect its confidentiality interests in this court.

1 item on any ground not addressed in this Stipulated Protective Order. Similarly, no Party waives any
2 right to object on any ground to use in evidence of any of the material covered by this Protective Order.

3 11.3 Copy of Order. When discovery is sought from a Non-Party in this action after entry of
4 this Order, a copy of this Order must accompany the discovery request.

5 11.4 Filing Protected Material. Without written permission from the Designating Party or a
6 court order secured after appropriate notice to all interested persons, a Party may not file in the public
7 record in this action any Protected Material. A Party that seeks to file under seal any Protected Material
8 must comply with Civil Local Rule 79-5. Protected Material may only be filed under seal pursuant to
9 a court order authorizing the sealing of the specific Protected Material at issue. Pursuant to Civil Local
10 Rule 79-5, a sealing order will issue only upon a request establishing that the Protected Material at
11 issue is privileged, protectable as a trade secret, or otherwise entitled to protection under the law. If a
12 Receiving Party's request to file Protected Material under seal pursuant to Civil Local Rule 79-5(e) is
13 denied by the court, then the Receiving Party may file the Protected Material in the public record
14 pursuant to Civil Local Rule 79-5(e)(2) unless otherwise instructed by the court.

15 11.5 Export Control. Disclosure of Protected Material shall be subject to all applicable laws
16 and regulations relating to the export of technical data contained in such Protected Material, including
17 the release of such technical data to foreign persons or nationals in the United States or elsewhere. The
18 Producing Party shall be responsible for identifying any such controlled technical data, and the
19 Receiving Party shall take measures necessary to ensure compliance.

20 **12. FINAL DISPOSITION**

21 Within 60 days after the final disposition of this action, as defined in paragraph 4, each
22 Receiving Party must return all Protected Material to the Producing Party or destroy such material. As
23 used in this subdivision, "all Protected Material" includes all copies, abstracts, compilations,
24 summaries, and any other format reproducing or capturing any of the Protected Material. Whether the
25 Protected Material is returned or destroyed, the Receiving Party must submit a written certification to
26 the Producing Party (and, if not the same person or entity, to the Designating Party) by the 60-day
27 deadline that (1) identifies (by category, where appropriate) all the Protected Material that was returned
28

1 or destroyed and (2) affirms that the Receiving Party has not retained any copies, abstracts,
2 compilations, summaries or any other format reproducing or capturing any of the Protected Material.
3 Notwithstanding this provision, Counsel otherwise authorized to received Protective Material pursuant
4 to this Order are entitled to retain an archival copy of all pleadings, motion papers, trial, deposition,
5 and hearing transcripts, legal memoranda, correspondence, deposition and trial exhibits, expert reports,
6 attorney work product, and consultant and Expert work product, even if such materials contain
7 Protected Material, with the exception of paper copies of source code. Any such archival copies that
8 contain or constitute Protected Material remain subject to this Protective Order as set forth in Section 4
9 (DURATION).

10 PURSUANT TO STIPULATION, IT IS SO ORDERED.

11
12 DATED: _____

13
14 _____
15 Hon. James Donato
16 United States District Judge
17
18
19
20
21
22
23
24
25
26
27
28

EXHIBIT A

ACKNOWLEDGMENT AND AGREEMENT TO BE BOUND

I, _____ [print or type full name], of _____ [print or type full address], declare under penalty of perjury that I have read in its entirety and understand the Stipulated Protective Order that was issued by the United States District Court for the Northern District of California on [date] in the case of *Klein v. Meta Platforms, Inc.*, Case No. 3:20-cv-08570-JD. I agree to comply with and to be bound by all the terms of this Stipulated Protective Order and I understand and acknowledge that failure to comply could expose me to sanctions and punishment in the nature of contempt. I solemnly promise that I will not disclose in any manner any information or item that is subject to this Stipulated Protective Order to any person or entity except in strict compliance with, and explicitly provided by, this Order.

I further agree to submit to the jurisdiction of the United States District Court for the Northern District of California for the purpose of enforcing the terms of this Stipulated Protective Order, even if such enforcement proceedings occur after termination of this action. I waive any right I may otherwise have to object to the jurisdiction of said court.

I hereby appoint _____ [print or type full name] of _____ [print or type full address and telephone number] as my California agent for service of process in connection with this action or any proceedings related to enforcement of this Stipulated Protective Order.

Date: _____

City and State where sworn and signed: _____

Printed name: _____
[printed name]

Signature: _____
[signature]

EXHIBIT B

IN-HOUSE COUNSEL AGREEMENT CONCERNING CONFIDENTIALITY

I, _____ [print or type full name], of _____ [print or type full address] am employed by _____ as _____.

I declare under penalty of perjury that I have read in its entirety and understand the Stipulated Protective Order that was issued by the United States District Court for the Northern District of California on [date] in the case of Klein v. Meta Platforms, Inc. Case No. 3:20-cv-08570-JD.

I agree to comply with and to be bound by all the terms of this Stipulated Protective Order and I understand and acknowledge that failure to comply could expose me to sanctions and punishment in the nature of contempt. I solemnly promise that I will not disclose in any manner any information or item that is subject to this Stipulated Protective Order to any person or entity except in strict compliance, and explicitly provided by, this Order.

I further agree to submit to the jurisdiction of the United States District Court for the Northern District of California for the purpose of enforcing the terms of this Stipulated Protective Order, even if such enforcement proceedings occur after termination of this action. I waive any right I may otherwise have to object to the jurisdiction of said court.

I hereby appoint _____ [print or type full name] of _____ [print or type full address and telephone number] as my California agent for service of process in connection with this action or any proceedings related to enforcement of this Stipulated Protective Order.

Date: _____

City and State where sworn and signed: _____

Printed name: _____
[printed name]

Signature: _____
[signature]

1 DATED: July 5, 2022

Respectfully submitted,

2 HAGENS BERMAN SOBOL SHAPIRO LLP

QUINN EMANUEL URQUHART &
SULLIVAN, LLP

3
4 By s/ Shana E. Scarlett
SHANA E. SCARLETT

By s/ Stephen A. Swedlow
STEPHEN A. SWEDLOW

5 Shana E. Scarlett (SBN 217895)
6 715 Hearst Avenue, Suite 202
7 Berkeley, CA 94710
8 Telephone: (510) 725-3000
9 Facsimile: (510) 725-3001
shanas@hbsslaw.com

Stephen A. Swedlow (admitted *pro hac vice*)
Michelle Schmit (admitted *pro hac vice*)
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606-1881
Telephone: (312) 705-7400
stephenswedlow@quinnemanuel.com
michelleschmit@quinnemanuel.com

10 Steve W. Berman (admitted *pro hac vice*)
11 HAGENS BERMAN SOBOL SHAPIRO LLP
12 1301 Second Avenue, Suite 2000
13 Seattle, WA 98101
14 Telephone: (206) 623-7292
15 Facsimile: (206) 623-0594
16 steve@hbsslaw.com

Kevin Y. Teruya (Bar No. 235916)
Adam B. Wolfson (Bar No. 262125)
Brantley I. Pepperman (Bar No. 322057)
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
865 South Figueroa Street, 10th Floor
Los Angeles, CA 90017-2543
Telephone: (213) 443-3000
kevinteruya@quinnemanuel.com
adamwolfson@quinnemanuel.com
brantleypepperman@quinnemanuel.com

17 Manisha M. Sheth (admitted *pro hac vice*)
18 QUINN EMANUEL URQUHART &
19 SULLIVAN, LLP
20 51 Madison Avenue, 22nd Floor
21 New York, NY 10010
22 Telephone: (212) 849-7000
23 manishasheth@quinnemanuel.com

Interim Co-Lead Counsel for Consumer Class

W. Joseph Bruckner (admitted *pro hac vice*)
Robert K. Shelquist (admitted *pro hac vice*)
Brian D. Clark (admitted *pro hac vice*)
Rebecca A. Peterson (SBN 241858)
Arielle S. Wagner (admitted *pro hac vice*)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
wjbruckner@locklaw.com
rkshelquist@locklaw.com
bdclark@locklaw.com
rapeterson@locklaw.com
aswagner@locklaw.com

Executive Committee for Consumer Class

SCOTT + SCOTT ATTORNEYS AT LAW LLP

BATHAE DUNNE LLP

By: /s/ Kristen M. Anderson
Kristen M. Anderson (Bar No. 246108)
kanderson@scott-scott.com
230 Park Avenue, 17th Floor
New York, NY 10169
(212) 223-6444

By: /s/ Yavar Bathae
Yavar Bathae (Bar No. 282388)
yavar@bathaeedunne.com
Andrew C. Wolinsky (*pro hac vice*)
awolinsky@bathaeedunne.com
445 Park Avenue, 9th Floor
New York, NY 10022
(332) 322-8835

Christopher M. Burke (Bar No. 214799)
cburke@scott-scott.com
David H. Goldberger (Bar No. 225869)
dgoldberger@scott-scott.com
Hal D. Cunningham (Bar No. 243048)
hcunningham@scott-scott.com
Daniel J. Brockwell (Bar No. 335983)
dbrockwell@scott-scott.com
Yifan (Kate) Lv (Bar No. 302704)
klv@scott-scott.com
600 W. Broadway, Suite 3300
San Diego, CA 92101
(619) 233-4565

Brian J. Dunne (Bar No. 275689)
bdunne@bathaeedunne.com
633 West Fifth Street, 26th Floor
Los Angeles, CA 90071
(213) 462-2772

Edward M. Grauman (*pro hac vice*)
egrauman@bathaeedunne.com
7000 North MoPac Expressway, Suite 200
Austin, TX 78731
(512) 575-8848

*Interim Co-Lead Counsel for the Advertiser
Classes*

Patrick J. McGahan (*pro hac vice*)
pmcgahan@scott-scott.com
Michael P. Srodoski (*pro hac vice*)
msrodoski@scott-scott.com
156 South Main Street, P.O. Box 192
Colchester, CT 06415
(860) 537-5537

*Interim Co-Lead Counsel for the Advertiser
Classes*

AHDOOT & WOLFSON, PC
Tina Wolfson (Bar No. 174806)
twolfson@ahdootwolfson.com
Robert Ahdoot (Bar No. 172098)
rahdoot@ahdootwolfson.com
Theodore W. Maya (Bar No. 223242)
tmaya@ahdootwolfson.com
Henry Kelston (*pro hac vice*)
hkelston@ahdootwolfson.com
2600 West Olive Avenue, Suite 500
Burbank, CA 91505
(310) 474-9111

*Executive Committee Counsel for the
Advertiser Classes*

LEVIN SEDRAN & BERMAN LLP
Keith J. Verrier (admitted *pro hac vice*)
kverrier@lfsblaw.com
Austin B. Cohen (admitted *pro hac vice*)
acohen@lfsblaw.com
510 Walnut Street, Suite 500
Philadelphia, PA 19106-3997
(215) 592-1500

*Executive Committee Counsel for the Advertiser
Classes*

By: /s/ Sonal N. Mehta
**WILMER CUTLER PICKERING HALE AND
DORR LLP**
SONAL N. MEHTA (Bar No. 222086)
Sonal.Mehta@wilmerhale.com
2600 El Camino Real, Suite 400
Palo Alto, California 94306
Telephone: (650) 858-6000

DAVID Z. GRINGER (*pro hac vice*)
David.Gringer@wilmerhale.com
7 World Trade Center
250 Greenwich Street
New York, New York 10007
Telephone: (212) 230-8800

ARI HOLTZBLATT (*pro hac vice*)
Ari.Holtzblatt@wilmerhale.com
MOLLY M. JENNINGS (*pro hac vice*)
Molly.Jennings@wilmerhale.com
1875 Pennsylvania Ave NW
Washington, DC 20006
Telephone: (202) 663-6000

Attorneys for Defendant Meta Platforms, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on July 5, 2022, the foregoing document was transmitted to the Clerk's Office using the CM/ECF System, causing the document to be electronically served on all attorneys of record.

Dated: July 5, 2022

By s/ Shana E. Scarlett
Shana E. Scarlett

ATTACHMENT D**DEFINITIONS AND INSTRUCTIONS**

1
2
3 1. In answering each request, You are commanded to furnish all documents, however
4 held or obtained, that are in Your possession, custody, or control — including, but not limited to,
5 legal (de jure), actual (de facto), constructive, and practical possession, custody, or control of Your
6 officers, directors, employees, contractors, counsel, auditors, insurers, investigators, consultants,
7 agents, or other representatives acting for or on Your behalf, or that are maintained in Your records,
8 including, but not limited to, documents obtained through discovery in this or any other litigation.
9 For the avoidance of doubt, You shall not be commanded to furnish documents that are in the
10 possession or custody of any of Your subsidiaries domiciled in the United States.

11 2. “Daily Active Users” means users who maintain active accounts on a daily basis or
12 who use the product at least once per day.

13 3. “Executives” means Your Chief Executive Officer, Chief Financial Officer, Chief
14 Operating Officer, Chief Product Officer, Chief Technology Officer, or Chief Marketing Officer.

15 4. “Telegram” means the software application known publicly as “Telegram,”
16 released initially in or around August 2013, and owned and operated by Telegram Messenger.

17 5. “Telegram Messenger,” the “Company,” or “You” or “Yours” means Telegram
18 Messenger Inc., a corporation, its wholly or partially owned subsidiaries, parent companies,
19 unincorporated divisions, joint ventures, partnerships, operations under assumed names,
20 predecessors, affiliates, investment vehicles, and all directors, officers, partners, employees,
21 agents, attorneys, consultants, and any other Person or entity, working for or on behalf of any of
22 the foregoing.
23
24
25
26
27
28

1 **DOCUMENTS REQUIRED TO BE PRODUCED**

2 **REQUEST FOR PRODUCTION NO. 1:**

3 Presentations or memoranda to the board of directors or Executives from August 1, 2013
4 to July 31, 2016, and from January 1, 2021 to December 31, 2021, discussing or analyzing
5 competition between Telegram and Facebook, Instagram, or WhatsApp.

6 **REQUEST FOR PRODUCTION NO. 2:**

7 Presentations or memoranda to Executives or the board of directors from August 1, 2013
8 to July 31, 2016, and from January 1, 2021 to December 31, 2021, indicating whether, or the extent
9 to which, Telegram is used to maintain personal relationships and share experiences with friends,
10 family, and other personal connections.

11 **REQUEST FOR PRODUCTION NO. 3:**

12 Presentations or memoranda to Executives or the board of directors from August 1, 2013
13 to July 31, 2016, and from January 1, 2021 to December 31, 2021, discussing compensation of
14 Telegram users for their use of Telegram. If there are no responsive documents, please provide a
15 statement to that effect.

16 **REQUEST FOR PRODUCTION NO. 4:**

17 Presentations or memoranda to Executives or the board of directors from August 1, 2013
18 to July 31, 2016, and from January 1, 2021 to December 31, 2021, relating to Telegram
19 Messenger's use of its privacy policies or privacy practices as a means of product differentiation
20 or to gain a competitive advantage over any other firm's Product(s), including Meta's Products.
21 If there are no responsive documents, please provide a statement to that effect.

22 **REQUEST FOR PRODUCTION NO. 5:**

23 Presentations or memoranda to Executives or the board of directors from January 1, 2011
24 to December 31, 2014, and from January 1, 2021 to December 31, 2021, that discuss or analyze
25 the impact of privacy policies or privacy practices on user satisfaction or engagement.

26 **REQUEST FOR PRODUCTION NO. 6:**

1 Documents or data identifying, on an hourly and daily basis, from September 27, 2021 to
2 October 18, 2021, the number of active users, the total amount of time spent, and the average
3 amount of time spent per user on Telegram, for each country in which Telegram is offered.

4 **REQUEST FOR PRODUCTION NO. 7:**

5 Documents or data identifying the number of Daily Active Users of Telegram and the
6 average amount of time spent per Daily Active User on Telegram generated or available on a
7 weekly, monthly, and annual basis from August 1, 2013 to July 31, 2016, and from January 1,
8 2021 to December 31, 2021, for each country in which Telegram is offered.